THE UNIVERSITY of ADELAIDE

A Deep Dive into the Socio-Technical Aspects of Delays in Security Patching

Ali Babar

CREST – Centre for Research on Engineering Software Technologies

Monash Cybersecurity Seminar, 18th October, 2022

Equifax – A Credit Assessment Service

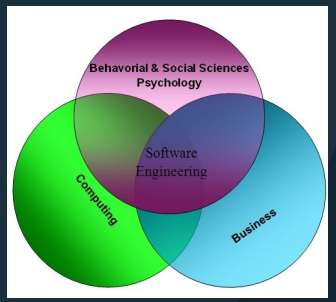
NHS – A Health Service Agency

Optus – A Telco

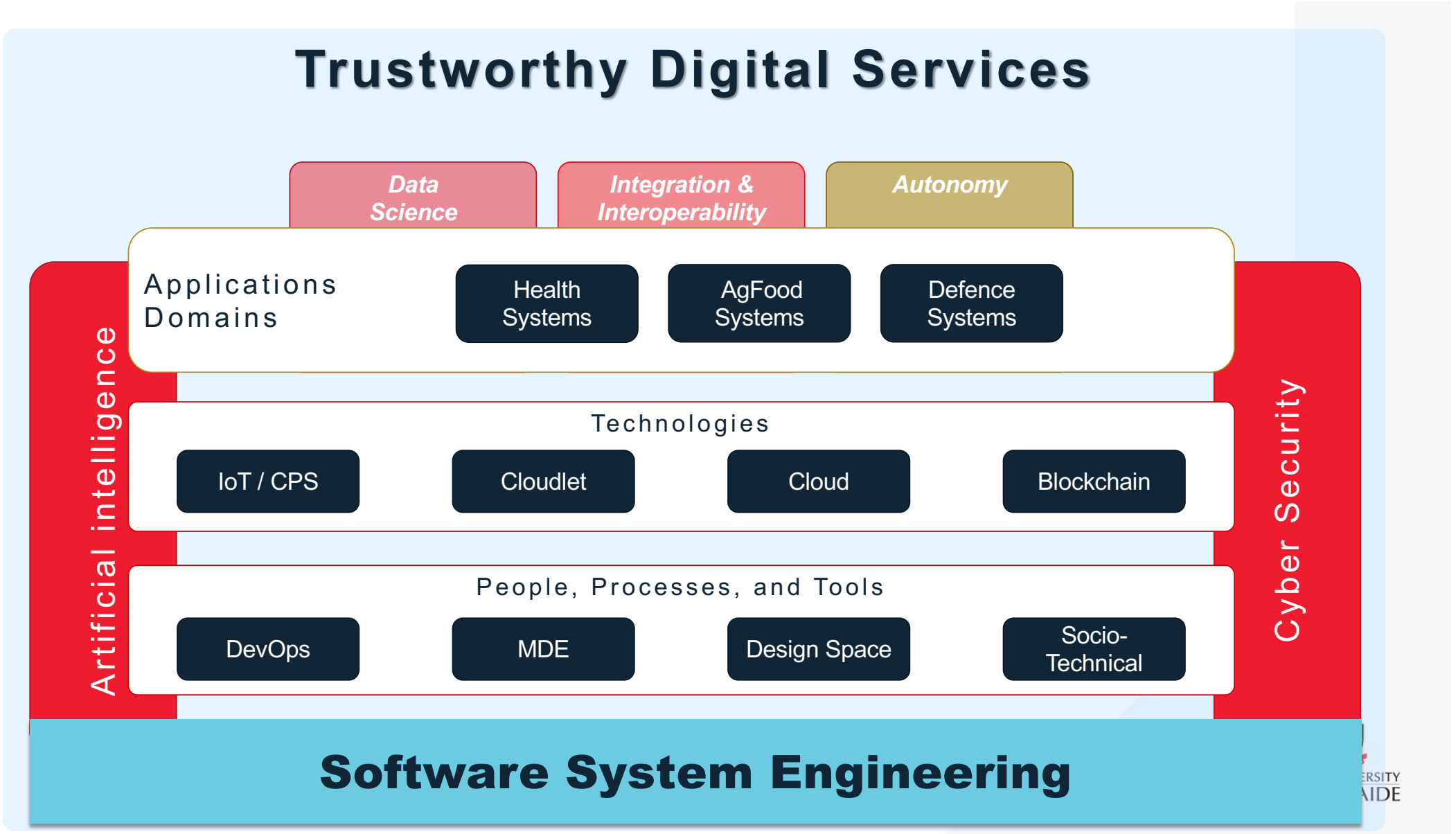
Brief Bio

M. Ali Babar

- Cyber Security Cooperative Research Centre (CSCRC) – Jemena, ACTewAGL, TCS, Cisco, NAB, Defence SA, SA Health, Q-Labs, WA DGov, SA Gov, TSS and ATO
- Lancaster – CPNI/GCHQ
- Denmark – Danish Strategic funding agency (5 industry partners)
- Lero, Ireland – focused on Irish industry scaling to Robert Bosch, Finnish industry
- NICTA – CeBIT, DSTG, Mini MBA
- JRCASE - CSIRO-MacQ Uni – Linkage project



THE UNIVERSITY of ADELAIDE


Trustworthy Digital Services
Data Science
Integration & Interoperability
Autonomy
Applications Domains
Health Systems
AgFood Systems
Defence Systems
Technologies
IoT / CPS
Cloudlet
Cloud
Blockchain
People, Processes, and Tools
DevOps
MDE
Design Space
Socio-Technical
Artificial intelligence
Cyber Security
Software System Engineering

Talk's Roadmap

- Setting the context of our research
- Security Patch management as a socio-technical system
- Research questions stimulating our studies on this topic
- Methodological and logistical details
- Taxonomy of reasons for delays in security patching
- Strategies to avoid/minimize delays
- Takeaways for practitioners and researchers

THE UNIVERSITY of ADELAIDE

Setting the Context – Problem Statement

ars TECHNICA

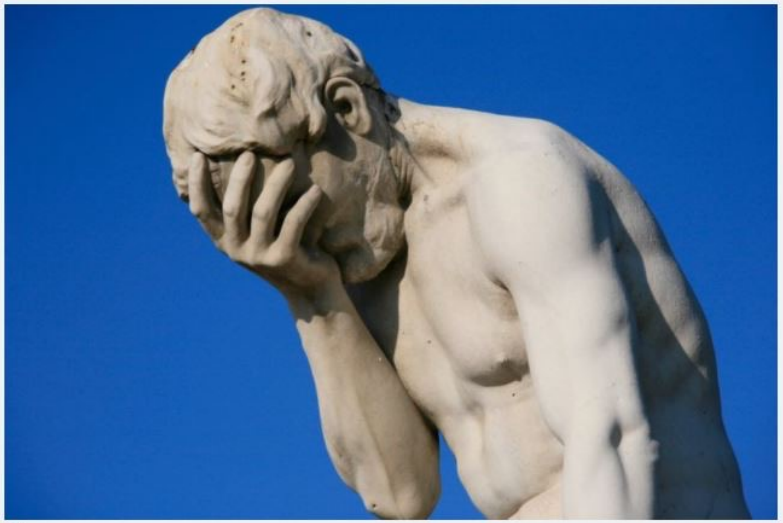
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

BIZ & IT —

Failure to patch two-month-old bug led to massive Equifax breach

Critical Apache Struts bug was fixed in March. In May, it bit ~143 million US consumers.

DAN GOODIN - 9/14/2017, 12:42 PM



Wikimedia Commons/Alex E. Proimos

Enlarge

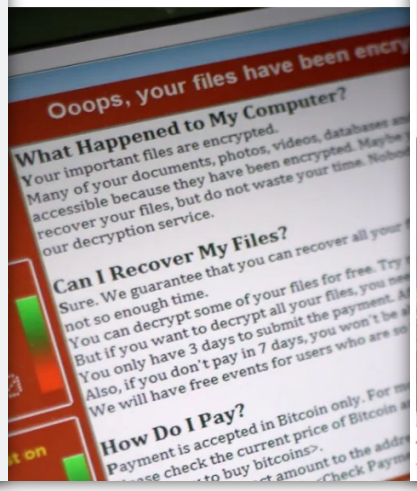
237

The Equifax breach that exposed sensitive data for as many as 143 million US consumers was accomplished by exploiting a Web application vulnerability that had been patched more than two months earlier, officials with the credit reporting service said Thursday.

fter WannaCry, a millio sk

the leaked NSA tools remains a conce

7:07 am ACST • May 13, 2019



The New York Times

Cyber Attack Suspected in German Woman's Death

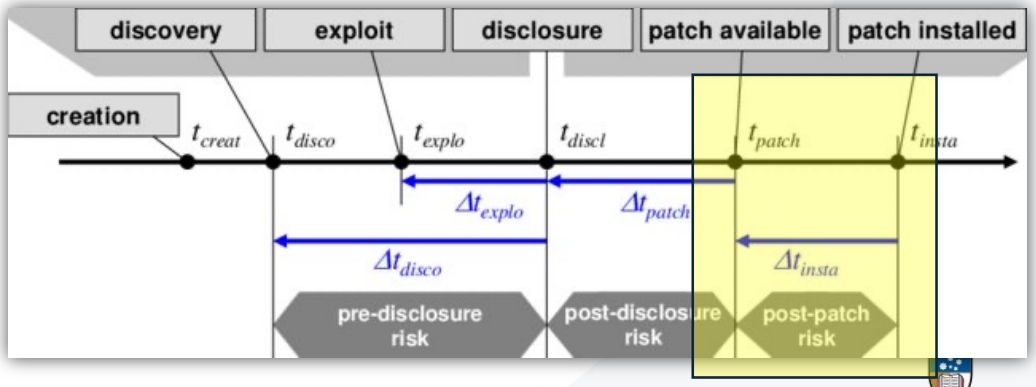
Prosecutors believe the woman died from delayed treatment after hackers attacked a hospital's computers. It could be the first fatality from a ransomware attack.

The ransomware attack involved servers at the University Hospital Düsseldorf on Sept. 10. Roland Weihrauch/dpa, via ZUMA Press

https://techcrunch.com/2019/05/12/wannacry-two-years-on/?guccounter
https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/
https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html?smid=tw-share

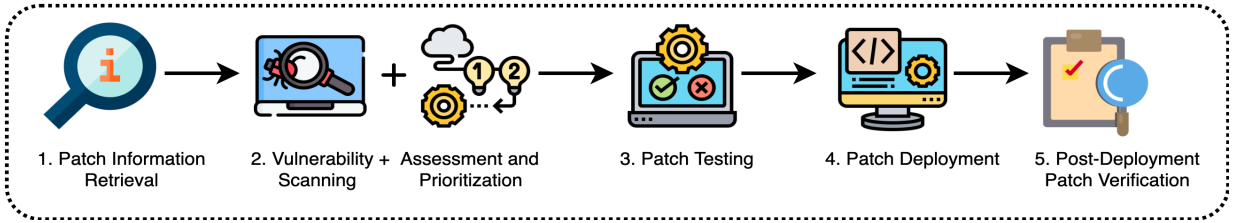
Setting the Context - Security Patch Management

The **application of security patches** to address the identified security vulnerabilities in the software code



M. Souppaya, K. Scarfone, Guide to enterprise patch management technologies, NIST Special Publica-1060tion 800 (2013) 40.
S. Frei et al., Modeling the security ecosystem-the dynamics of (in) security, Economics of Information Security and Privacy, Springer, Boston, MA, 2010

Security Patch Management Process



Retrieving new patches

- Proactive search for new patches
- Download patches

Deciding to patch

- Scan systems for vulnerabilities
- Decide relevance to managed systems
- Patch type and severity
- Organization policies/compliance (e.g., Change Management)

Preparing for patch installation

- Patch pre-requisite investigation
- Make backups or snapshots
- Prepare machines (e.g., configurations, patch dependencies)
- Patch testing

Installing patches

- Time update to avoid disruptions
- Coordinate with stakeholders
- Receive organization approval
- Manual/automatic deployment

Handling post-deployment issues

- Monitor patch status
- Gather client feedback
- Decision by organization policy
- Uninstall patch
- Revert to prior software version
- Find workaround/ troubleshoot

F. Li et al., Keepers of the machines: examining how system administrators manage software updates. USENIX Conference on Usable Privacy and Security, 2019.
C. Tiefenau et al., Security, Availability, and Multiple Information Sources: Exploring Update Behavior of System Administrators. In Sixteenth Symposium on Usable Privacy and Security ({SOUPS} 2020).

THE UNIVERSITY of ADELAIDE

Security Patching as a Socio-Technical System

- Emery & Trist coined the term,1960, socio-technical system: a system with a complex interaction between humans, machines and context
- Such system has many interdependent internal and external parts to be considered within their context
- Designers/engineers can avail more than one paths to reach the system's goals – design choices
- System performance is dependent upon a combination of technical and social subsystems; ignore one results in poor outcomes

Baxter & Sommerville, From design methods to systems engineering, Interacting with Computers, 23 (2011) 4-17

THE UNIVERSITY of ADELAIDE

What did Stimulate our Studies on this Topic

- Why, how and where do delays occur in software security patch management?
- How can the delays be mitigated?
- How are the interdependent activities coordinated?
- Is there any underlying theoretical model of coordinating the socio-technical interactions/decisions?
- What are the automation needs and how to meet them?
- How would human-automation support work?

THE UNIVERSITY of ADELAIDE

Finding Some Answers

Methodological and Logistical Details

Methodological Details – Data Collection (1/2)

Observations

- 51 patch meetings
- March 2020 - January 2021
- 2 organizations, 8 teams
- 90 min (avg), online meetings

Post-meeting Discussions

- 11 discussions
- 30 - 45 mins (avg)

Artifacts Analysis

- Patch meeting minutes
- Patch mailing thread

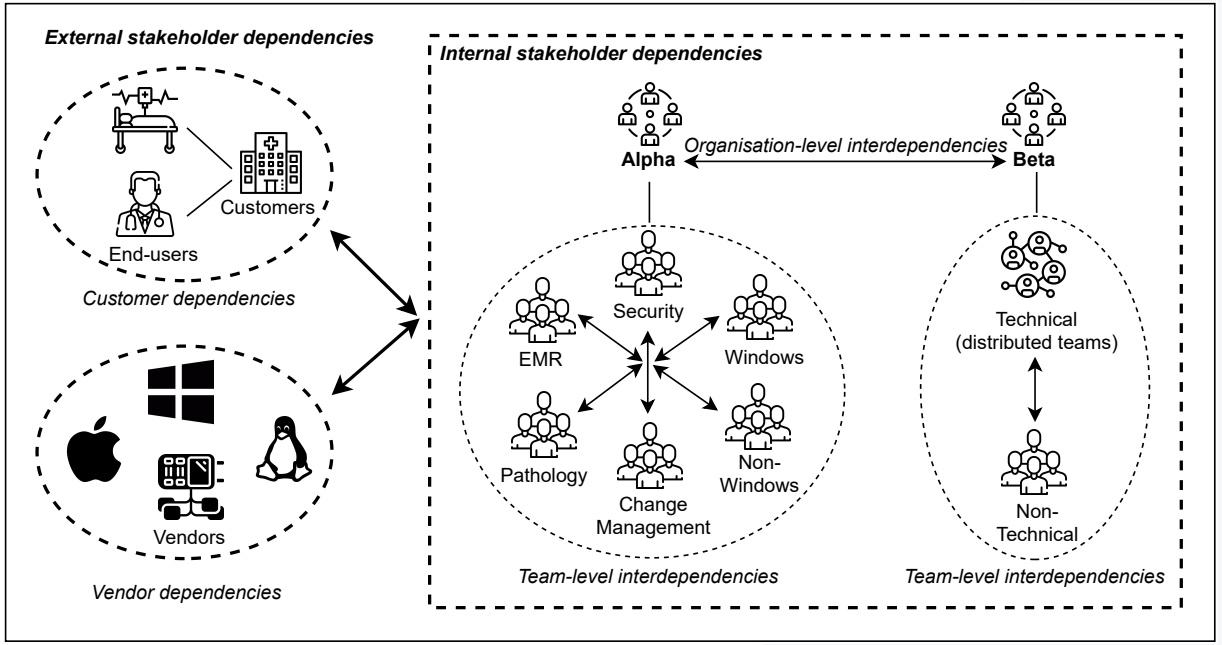
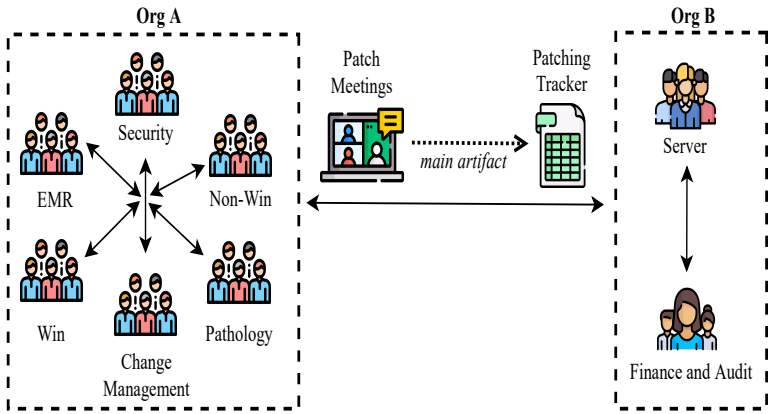


Figure: The studied context

THE UNIVERSITY of ADELAIDE

Methodological Details – Data Collection (2/2)



Analysis of patching tracker

Total no. of tasks = 232
No. of delayed tasks = 131 (56.5%)

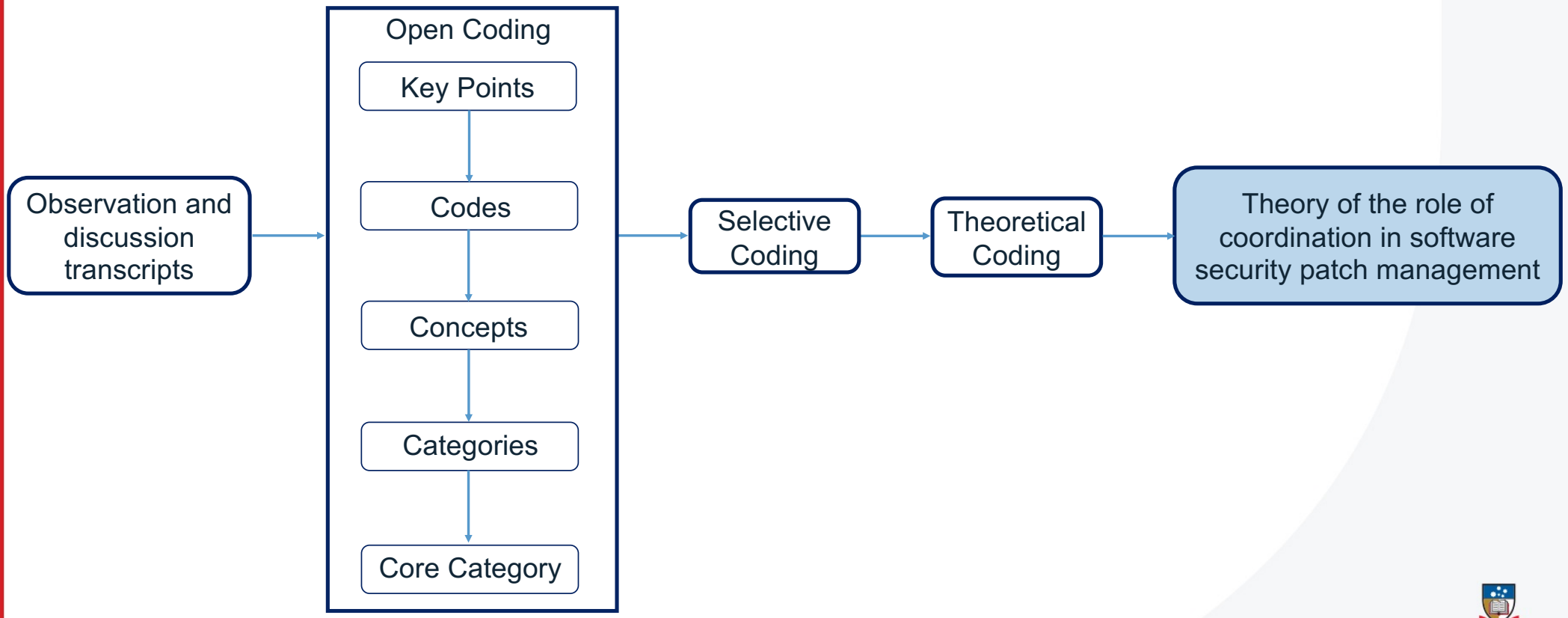
Id	Raised on	Task No	PM Phase	Subject	Action Required/Taken	Raised By	Owner	Assigned To	Status	Start Date	End Date	Actual Duration	Planned duration	Difference
1	29-Jun-18	1	Vulnerability Scanning & Assessment and Prioritization	IE7 and IE8 needs to be upgraded on win2008 servers to IE11	7/9 - quote now with Team T1 to approve. 19/10 - [P1] to confirm quote is approved and IE11 uprgade can go ahead. Org B to provide list of servers with non IE11.	Org B	Org A	P1	Closed	29-Jun-18	23-May-19	11 months	1 week	10.75 months
2	27-Jul-18	2	Patch Testing	NSSR to be raised by Team T1 to get Service Packs (various products) updated as many patches cannot apply due to	27/7 - [P1] will send report from Shavlik showing what the missing Service Packs are as they relate to different product levels. 31/7/18 - SP report sent to [P2] via	Org B	Org A	P2	Closed	27-Jul-18	31-Jul-19	12 months	1 week	11.75 months
3	26-Oct-16	70	Patch Deployment	Country servers - [s1] - patch via USB - Shavlik agent installation Task [T1]	ISSUE - deploying patching is too slow, going outside patch window. Suggest deployng agent to those as is the Ivanti recommendation for remote	Org A	Org B	P2	Closed	26-Oct-16	17-May-17	7 months	2 weeks	6.5 months

Table 2. Definition of standard time frames in the studied organisation

Phase ID	Patch management process phase	Standard time frame	Note
P1	Patch Information Retrieval	2 days	Needs to be completed within two days of patch release
P2	Vulnerability Scanning, Assessment and Prioritisation	1 week	Needs to be completed within the first week of patch release
P3	Patch Testing	1 week	Needs to be completed within the second week of patch release
P4	Patch Deployment	2 weeks	Needs to be completed within the fourth week of patch release
P5	Post-Deployment Patch Verification	1 month	Any post-deployment issues must be resolved by the next patch cycle

THE UNIVERSITY of ADELAIDE

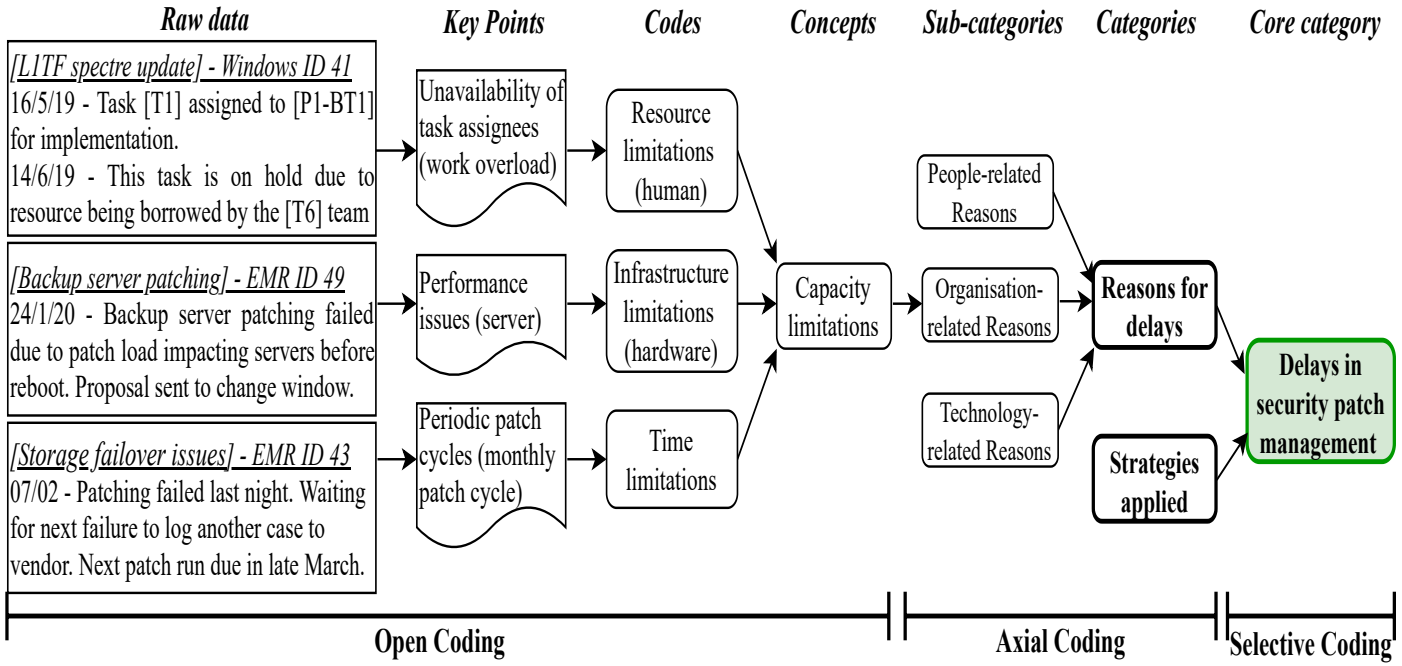
Methodological Details – Data Analysis Stages



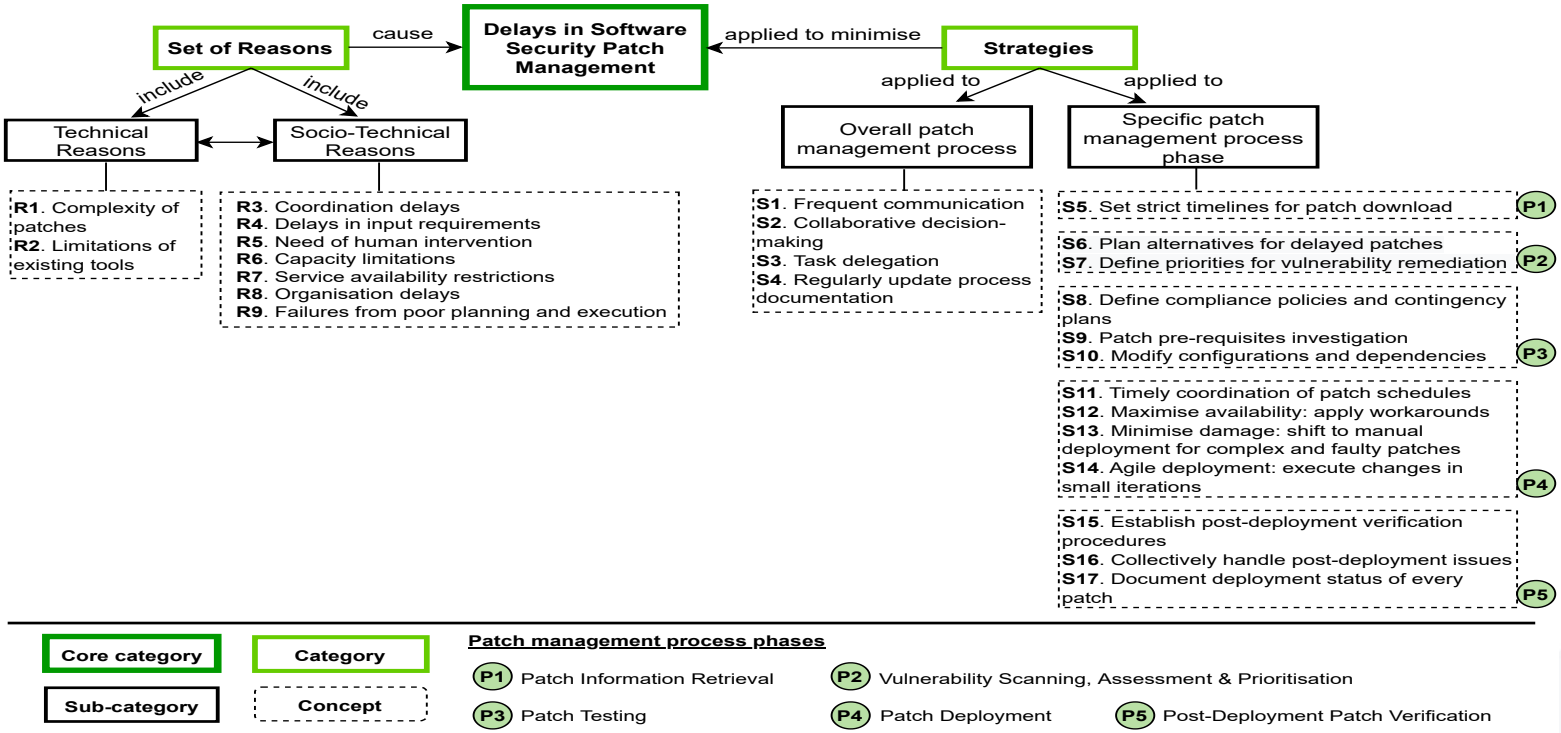
Glaser's **Grounded Theory** data analysis procedure

THE UNIVERSITY of ADELAIDE

Methodological Details – Data Analysis Example



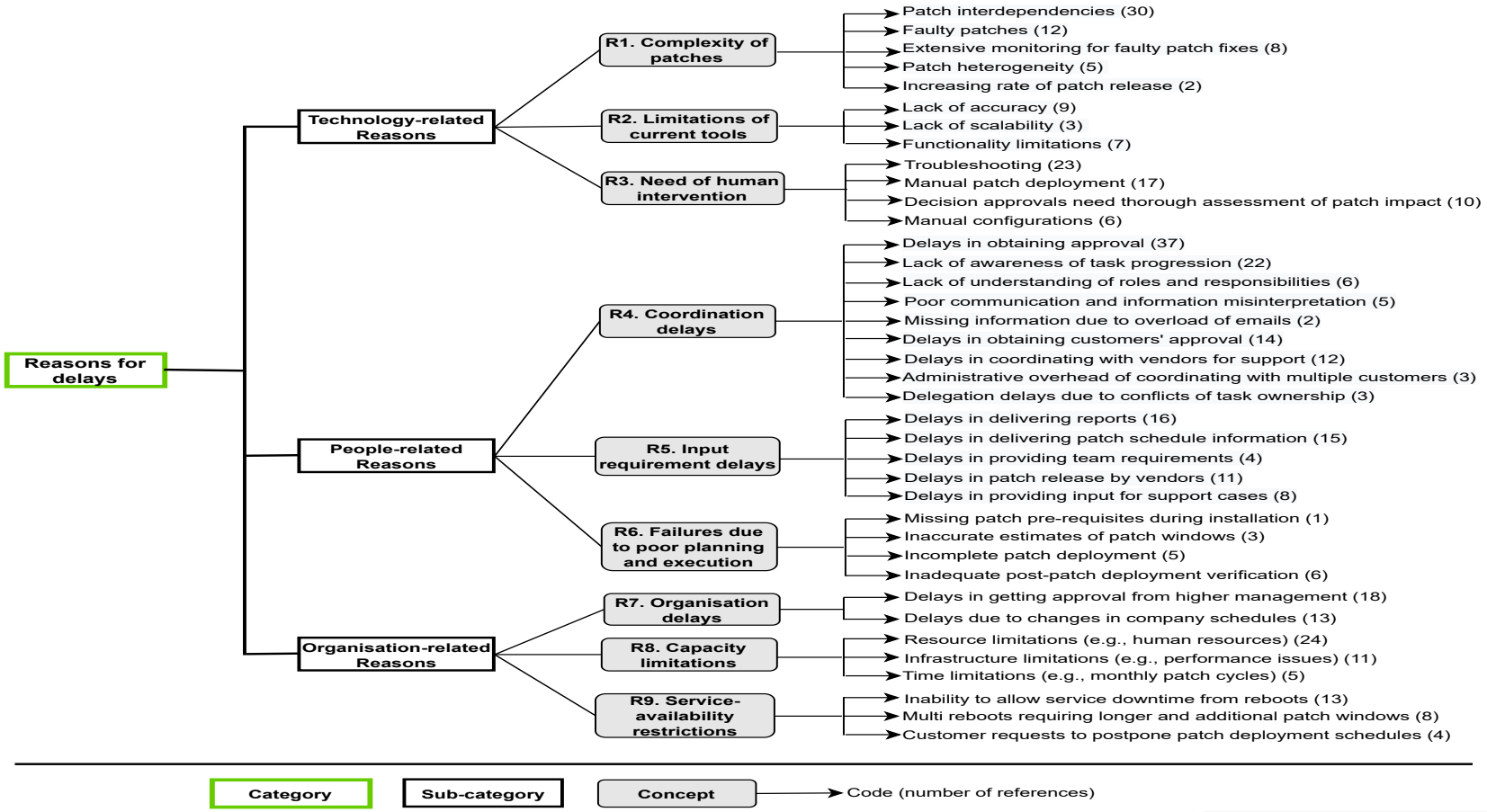
An Overview of the Key Aspects of Study



THE UNIVERSITY of ADELAIDE

Why, How and Where of Delays in Software Security Patch Management

A Taxonomy of the Identified Reasons for Delays



THE UNIVERSITY of ADELAIDE

TR1: Delays Caused by Complexity of Patches

- Detecting and dealing with patch interdependencies – software, hardware and firmware of new & legacy systems (1.5K Servers)
- Faulty patches causing unknown errors during patch testing, deployment, and post-deployment
- Security patches usually require extensive post-deployment monitoring to verify the fixes
- Frequent release of patches and their heterogeneity add to the complexity of patches

THE UNIVERSITY of ADELAIDE

TR2: Delays Caused by Limitations of Tools

- Lack of accuracy in the output of current tools (e.g., missing some vulnerabilities during scanning, omitting patches during patch deployment) – ASE 2022 paper (more details)
- Lack of scalability to handle diverse types of patches and their features – disabling some of the tools' functionalities
- Inability to detect patch compatibility and the lack of capability to detect multi-reboot requirements

[Subject - Additional reboot required for .NET patching]

"7/2/20 - An investigation is needed around the number of required reboots for EMR patching and window requirements as a result if more reboots are required. A new process needs to be fleshed out when patching is postponed to accommodate the identification of the number of reboots required." - EMR, Task ID 35

THE UNIVERSITY of ADELAIDE

TR3: Delays Caused by Need of Human Intervention

- Human intervention emerges as full automation not available or desirable – faulty patches causing unknown errors
- Manual configurations for selecting a suitable Group Policy Object (GPO) configurations to avoid breakdowns
- Human support may be needed for deploying complex, erroneous or business-critical patch installations, e.g., legacy systems
- Manual intervention for re-executing failed patch deployments and re-planning patch schedules due to requirement changes.

31/10/19 - [B-T1] team putting in significant amounts of work, like 15-20 hours per month, to redo the schedules on custom dates each time the deployments move off standard windows." - EMR, Task ID 30

THE UNIVERSITY of ADELAIDE

PR4: Delays Caused by Coordination Issues

- A single patching task usually involves multiple interdependent activities and several stakeholders – internal and external
- A lack of awareness of task progression and of understanding of shared roles and responsibilities
- Email based communication about patches may result in lost and/or misinterpretation of critical information
- Customers, End-users, Vendors inefficiently coordinating for seeking and giving approvals for system downtime & verification
- FSE 2021 paper (More details)

THE UNIVERSITY of ADELAIDE

PR5: Delays Caused by Input Requirements Issues

- Tightly coupled activities have input requirements be fulfilled in timely fashion, e.g., vulnerability scan reports or prioritisation
- Non-delivery or incomplete delivery of the schedule-related information resulting in poor planning for deploying patches
- No online repository for maintaining servers' patching details
- Delays in receiving vendor's support for patching errors and new patch release information

[Subject - New zero-day vulnerability warning]

"12/6/20 - Monitor Microsoft patch release for critical vulnerability identified on [T1] servers. Font Type 1 expected as a zero-day soon, full report not available yet.

24/7/20 - No update from Microsoft." - EMR, Task ID 43

THE UNIVERSITY of ADELAIDE

PR6: Delays Caused by Poor Planning and Execution

- Security patch management needs meticulous planning and flawless execution to avoid system breakdowns
- Inaccurate estimates of patch windows may result in calling off the whole process as mission cannot put on hold
- Unforeseen errors can become major risks to deploying within the planned time frame if not considered during planning
- Incomplete patch deployment or insufficient verification needing re-execution of patch deployment and operational disruption

THE UNIVERSITY of ADELAIDE

OR7: Delays Caused by Policy & Procedures

- Ensuring full compliance with the organisational policies and obtaining management approval for monthly patch schedules

- Changes in organisation schedules such as change freeze periods, testing schedules like regression testing plans and shutdown periods

[Subject - Patching for December 2019]

“18/10/19 - OOB for November patching from 4th December instead of December patching. 31/10/19 - [AT1] patching for December month is off but November Microsoft patches will be applied in the first week of December instead to keep compliance up." - EMR, Issue ID 29

THE UNIVERSITY of ADELAIDE

OR8: Delays Caused by Capacity Limitations

- Lack/unavailability of qualified personnel experienced in handling specific systems for patching, e.g., legacy system upgrades
- Insufficient infrastructure resources - hardware and network limitations may hinder a patching task
- Testing the workarounds for failed deployments delayed for weeks given the time-driven (i.e., monthly) patch cycle

- **“24/1/20 - Patching cannot go ahead when the active backup is running. The patch load can impact servers before reboot. Need a window change, proposal to be sent by [P1-BT1] to [P2-AT1]." - EMR, Issue ID 39**

THE UNIVERSITY of ADELAIDE

OR9: Delays Caused by Service Level Agreements

- Organisations' inability to allow service downtime from reboots required for patches to take effect after deployment
- Multi reboots requirements difficult to get prompt approvals out of fear of service disruptions from longer patch windows
- Customers reluctant to agree to sufficiently large patch window; rather requesting service continuity at all cost

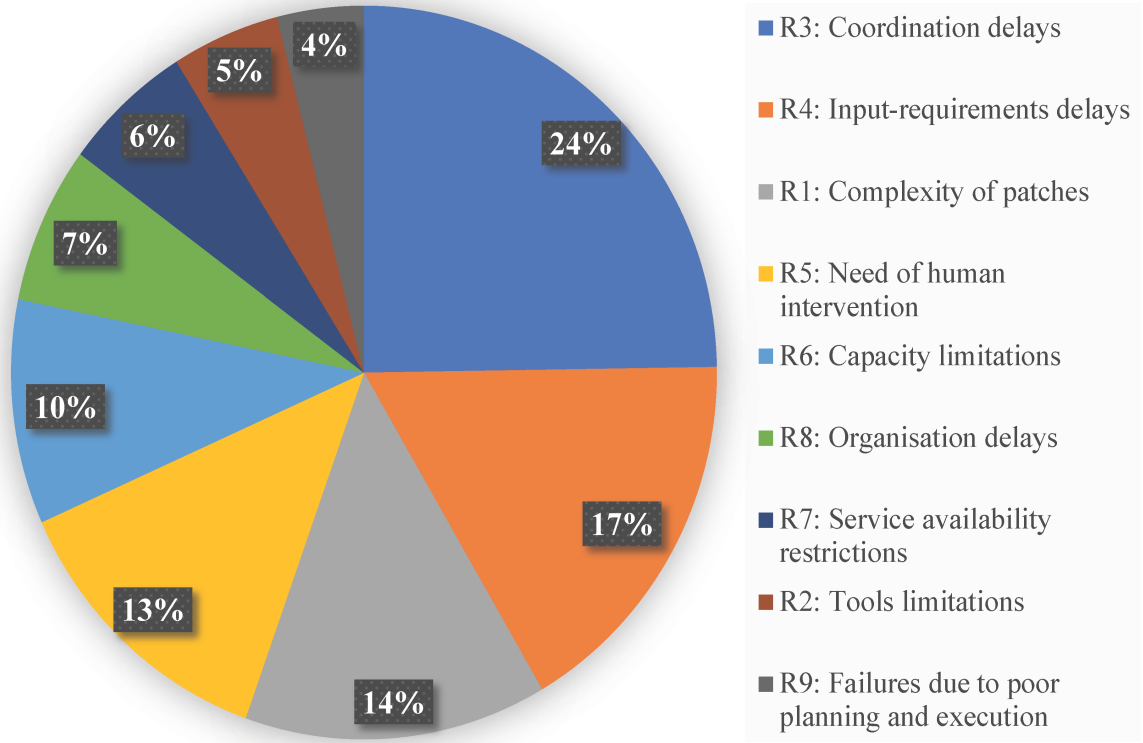
[Subject - [Servers s1 and s2] patching]

"26/7/19 - OOB window is needed for the multi reboots to catch up.

9/8/19 - Waiting for the customer's confirmation of the new patch window, pending information from [P1-AT1]." - EMR, Issue ID 20

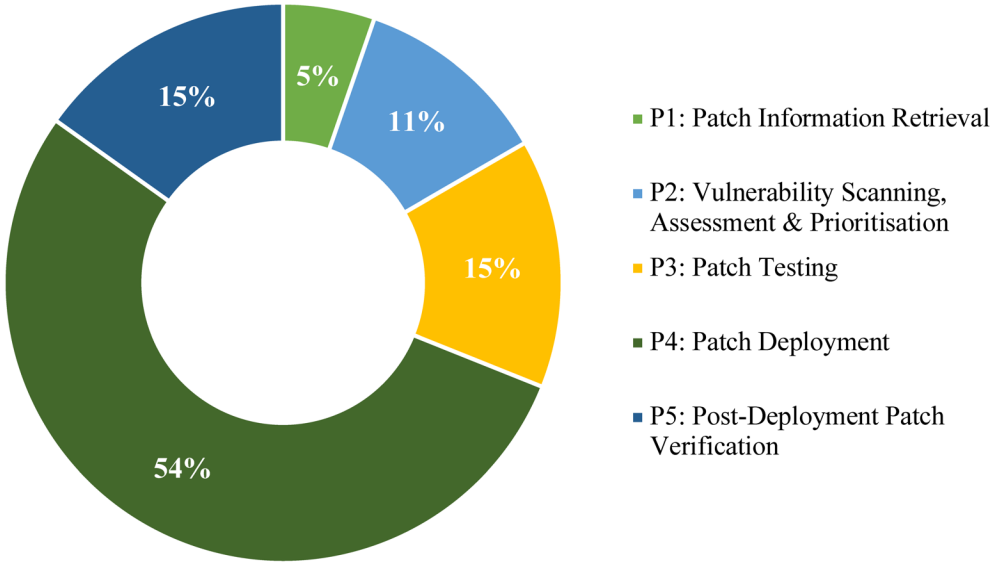
THE UNIVERSITY of ADELAIDE

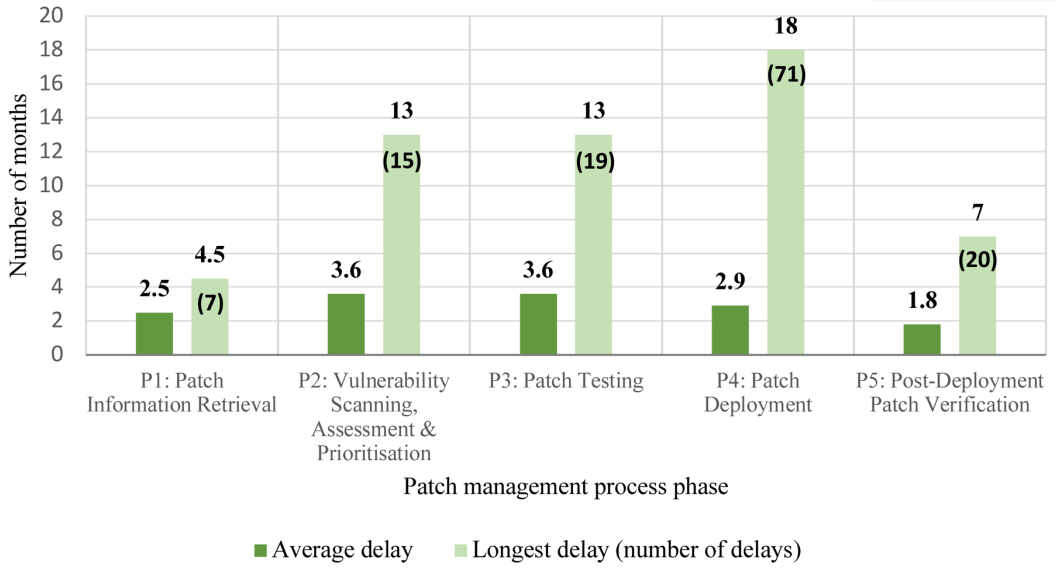
Frequency of Reasons for Delays



THE UNIVERSITY of ADELAIDE

Distribution of the Delays over the Process





THE UNIVERSITY of ADELAIDE

Strategies for Avoiding/Minimizing Delays

An Overview of the Used Strategies

Common strategies relating to the overall patch management process

S1. Frequent communication (24)
S2. Collaborative decision-making (3)
S3. Task delegation (31)
S4. Regularly review and update patch management process-related documentation (3)

Strategies relating to Patch Information Retrieval (P1)	Strategies relating to Vulnerability Scanning, Assessment & Prioritisation (P2)	Strategies relating to Patch Testing (P3)	Strategies relating to Patch Deployment (P4)	Strategies relating to Post-Deployment Patch Verification (P5)
S5. Set strict timelines for patch download (2)	**S6.** Plan alternatives for delayed patches (6) **S7**. Define priorities for vulnerability remediation (15)	**S8.** Define compliance policies and contingency plans for test failures (9) **S9**. Patch pre-requisites investigation (4) **S10**. Modify software configurations and dependencies (3)	**S11.** Timely coordination of patch deployment schedules (19) **S12**. Apply workarounds to maximise service availability (18) **S13.** Manual deployment for complex patches to minimise damage (12) **S14**. Agile deployment for executing changes (6)	**S15.** Establish post-deployment verification procedures (10) **S16**. Collectively handle post-deployment issues (9) **S17**. Document deployment status of every patch (3)

THE UNIVERSITY of ADELAIDE

Strategies – Patch Information Retrieval

- Setting tight timelines for patch download, e.g., within two days of the release of patch by the relevant vendors

- Acquiring and analysing the list of the retrieved patches each month before assessment and prioritisation of vulnerability

[Subject - Provide .NET report at the start of the patch cycle]

“15/3/19 - Org A requests BT1 to provide an extract of .NET released patches every month and a report including what patches will be applied to what servers." - EMR, Task ID 53

THE UNIVERSITY of ADELAIDE

Strategies – Vulnerabilities and Assessment

- Plan alternatives for scheduled patching based on assessment of the impact on other services and risks of cyber attacks
- Prioritised security patches based on the global vulnerability rating; High-risk vulnerabilities fixed within 48-72 hours
- Defining priorities for patching vulnerability for reducing the risk of exploitable attack vectors used successfully
- Prioritisation based on patch type – Patching OS earlier

[Subject - OS security patches need to be tracked separately in the vulnerability remediation]

"15/5/20 - [P1-AT1] requesting the OS security patches to be tracked separately from all other vulnerability remediation. Org B's report should only be addressing OS security patches anyway but can make sure to separate any non-OS remediation tasks." - EMR, Task ID 45

THE UNIVERSITY of ADELAIDE

Strategies – Patch Testing

- Test run compliance policies and standards, e.g., reboot every legacy server without patching; have contingency plans
- Allow a specific time to identify and modify the dependencies and configurations during patch testing
- Investigate the availability of prerequisites for the patches released every month as a separate task during patch testing

[Subject - Registry key missing for Knowledge Base (KB) ID [n] (LDAP)]

“2/10/20 - Patches not installed on [servers s1 and s2] due to missing a registry key. [P1-BT1] to check settings and apply where missing." - Win, Task ID 24

THE UNIVERSITY of ADELAIDE

Strategies – Patch Deployment

- Clustering similar patches to reduce the time spent in testing, deployment and rebooting
- Balancing workload on servers during patch deployment to avoid unnecessary service disruptions
- Backup servers concurrently running the critical services while being rebooted - Backup servers patched separately
- Manually patching business-critical servers having multiple version dependencies, multi reboots and legacy systems
- Agile deployment - execute the changes in small iterations

THE UNIVERSITY of ADELAIDE

Strategies – Post-Deployment Patch Verification

- Define a set of procedures for post-deployment patch verification to reduce the risk of delays caused by poor execution
- Monitor a patched system for functional, performance or unexpected issues; getting periodic scans to verify patching
- Collaborative problem handling for analysing the root causes for post-deployment issues and finding workarounds
- Develop a knowledge base to keep track of every patch as a reference in cases of errors encountered during the execution

[Subject - Automated second rescan for reboots]

"31/10/19 - [P1-BT1] raised this issue, he has configured the window to rescan for missing patches and conduct a second reboot if required. No issues during patching, seeking client feedback for verification." - EMR, Task ID 28

THE UNIVERSITY of ADELAIDE

Strategies – Overall Patch Management Process

- Frequent communication reduces delays, strengthens collaboration and improves mutual understanding
- Collectively making decisions about patch management helps teams gain insight into plans, activities and alternatives
- Well-defined roles and responsibilities around patch management activities resulting in delegation and accountability for actions
- Systematically and regularly review and update documents of patch actions and decisions; test execute process changes

“13/12/19 - Finalising the documentation after testing internally for handover to 24x7. 10/1/20 - Documentation to be tested in February, will be ready for handover in March." - EMR, Task ID 24

THE UNIVERSITY of ADELAIDE

Takeaways for Practitioners & Researchers

For Practitioners

- An understanding of the reasons for delays can enable security staff to take measures for mitigating the potential delays
- Provided knowledge can help practitioners in suitable decision-making, prioritisation and planning of patch management tasks
- Strategies can guide practitioners and organisations in better planning and taking actions to mitigate the impact of the delays
- Developing new and/or innovative use of existing tools for visualising dependencies, patch management knowledge repositories, timely communication and collaboration

THE UNIVERSITY of ADELAIDE

For Researchers

- Our findings are context and domain specific (healthcare) – extending and adapting case study for different domains
- Developing and executing interview guides and surveys to verify the findings and discover variations
- Research on AI-based tools for detecting patch mismatches, improved coordination across patching tasks and reducing delays
- Investigating the suitability of “human-AI collaboration" for security patch management
- Evaluating the performance and accuracy of available tools

THE UNIVERSITY of ADELAIDE

The Research Team

Nesara Dissanayake
@nesara_d

Asangi Jayatilaka
@DrAsangiJ

Mansooreh Zahedi
@MansoorehZ

Muhammad Ali Babar
@alibabar

Centre for Research on Engineering Software Technologies (CREST - @crest_uofa)
School of Computer Science, The University of Adelaide, Australia

CREST THE UNIVERSITY of ADELAIDE

Acknowledgements

- This talk is based on the research studies carried out by Nesara Dissanayake, M. Ali Babar, Mansooreh Zahedi, Asangi Asangi Jayatilaka

- Partially Funded by the University of Adelaide and the CREST

- SA Health provided the access to the case studies

- We are grateful to the participants for enabling to collect a variety of data for our research

THE UNIVERSITY of ADELAIDE

make history.

THE UNIVERSITY of ADELAIDE

CREST

Contact: Ali Babar
ali.babar@adelaide.edu.au

CYBER SECURITY COOPERATIVE RESEARCH CENTRE