

# Revision

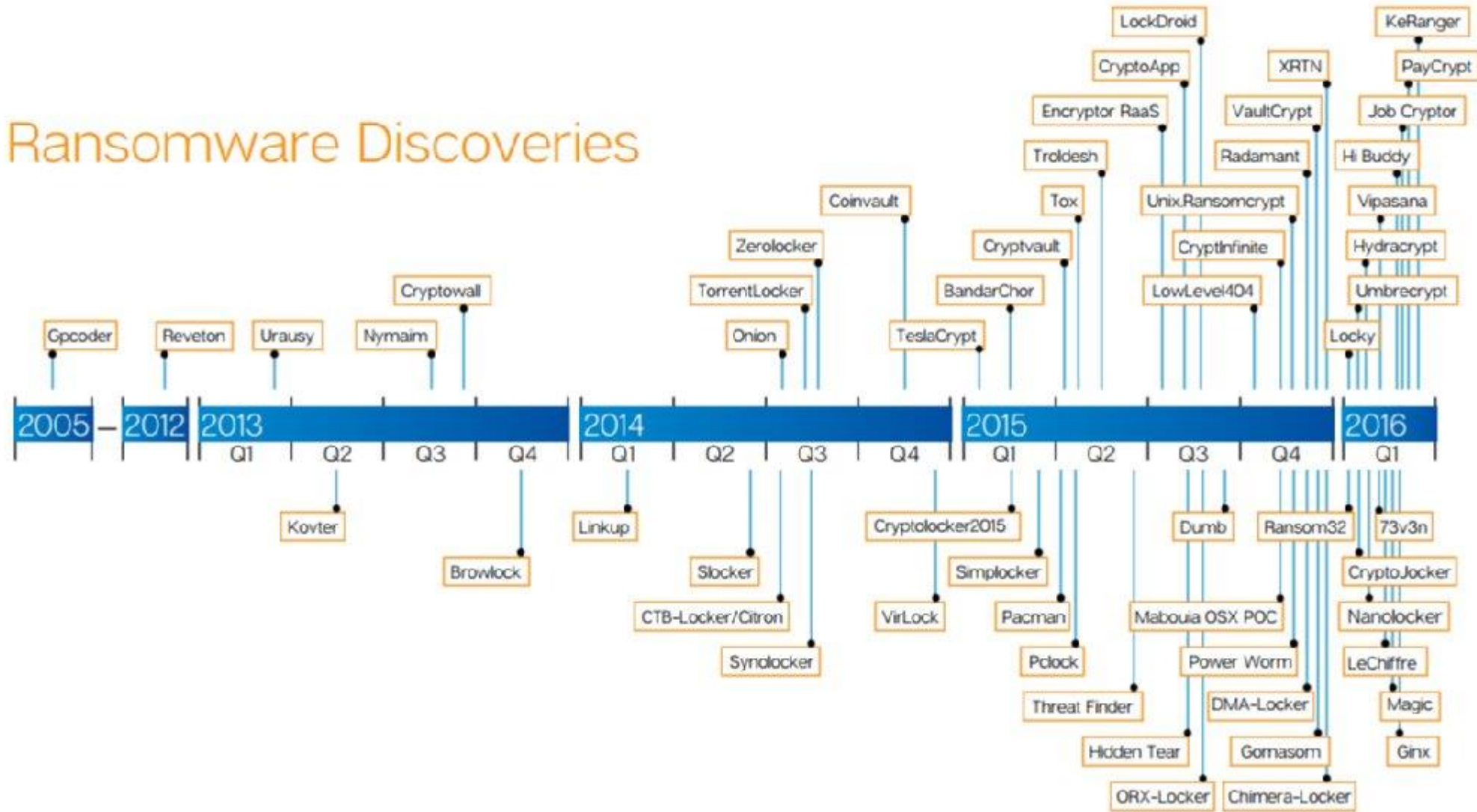
---

# First, the news ...

---

- Hospitals and ransomware
- <http://arstechnica.com/security/2016/02/la-hospital-latest-victim-of-targeted-crypto-ransomware-attack/>

# Ransomware Discoveries



# Security is a whole system issue

- Software
- Hardware
- Physical environment
- Personnel
- Corporate and legal structures

## Security properties to ensure

<b>Confidentiality</b>	No improper information gathering
<b>Integrity</b>	Data has not been (maliciously) altered
<b>Availability</b>	Data/services can be accessed as desired
<b>Accountability</b>	Actions are traceable to those responsible
<b>Authentication</b>	User or data origin accurately identifiable

# Cyber Security Essentials

- How might each of these protect against ransomware?



Secure configuration



Boundary firewalls and internet gateways



Access control and administrative privilege management



Patch management



Malware protection

# Access Control

# The problem: Backups at hospitals

---

- Hospitals need to backup data, but they also need to be certain that only the backup server is writing the data.
- Security lattices to the rescue...
- H: Classifications and linear ordering of classifications
- C: Categories
- Ordering:
  - $(h1, c1) \leq (h2, c2) \iff h1 \leq h2, c1 \subseteq c2$

Make this true:  
 $(h1, c1) \leq (h2, c2)$

$\iff$

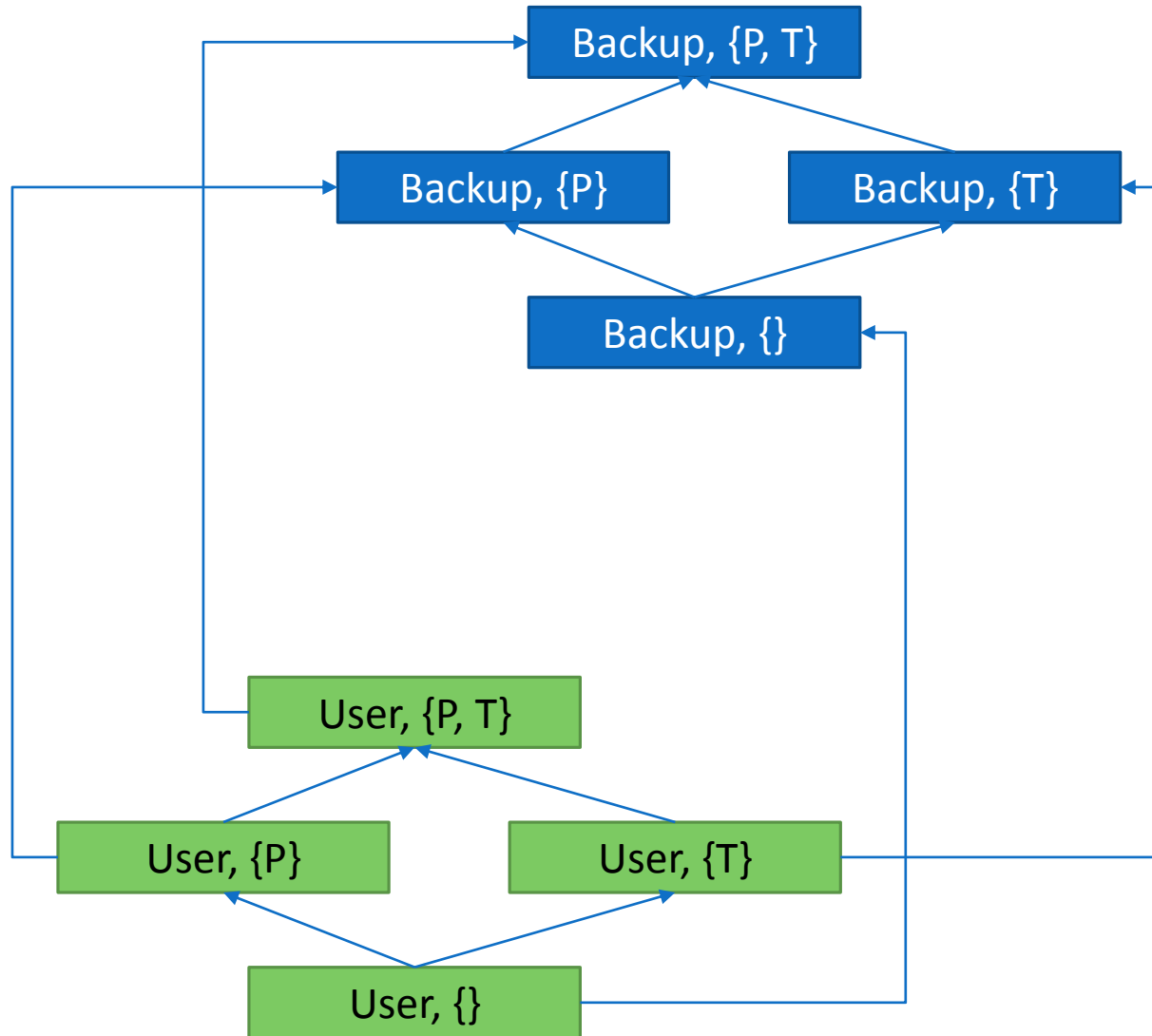
$h1 \leq h2, c1 \subseteq c2$

Classifications (H)

- Backup
- Users

Categories (C)

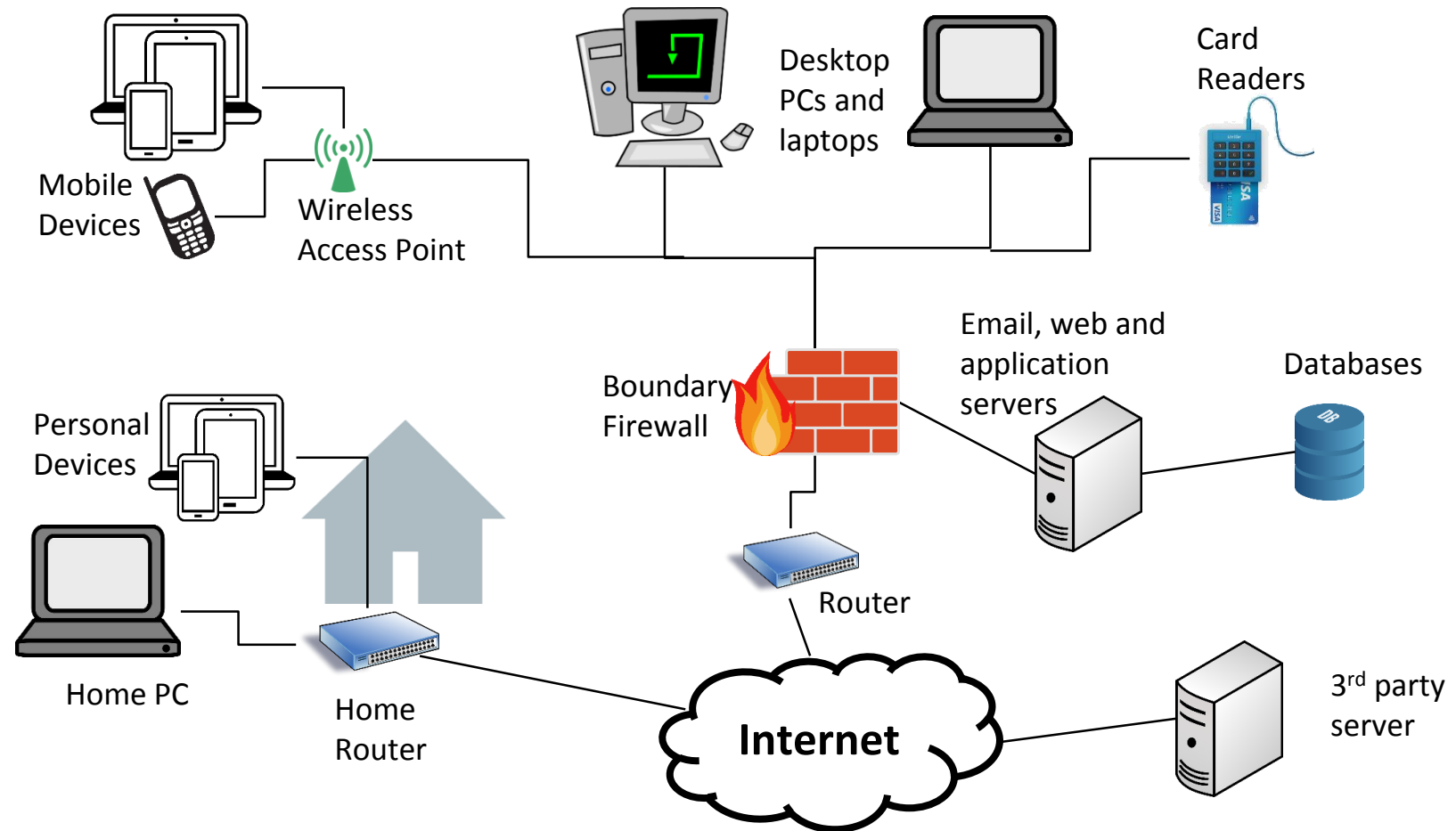
- P (Phyc ward)
- T (Transplant ward)





# Network attacks and defenses

- What needs to be protected from ransomware?
- How might Man-in-the-middle be used to add ransomware to a hospital network?
- How might a firewall be used to limit the spread of ransomware?



# Usable Security

# What on this email can be trusted?

From "Fletcher, Freya" <ffletcher@conejouisd.org> ☆

Subject **FW: ITS Administrative Support** 7:54 AM

To undisclosed-recipients; ☆ Other Actions ▾

---

**From:** Fletcher, Freya  
**Sent:** Thursday, March 05, 2015 4:47 AM  
**Subject:** ITS Administrative Support

Dear User,

Your password will expire within 24hrs Click on: [Staff & faculty update](#) to validate your e-mail.

This email has been scanned by the Symantec Email Security.cloud service.  
For more information please visit <http://www.symanteccloud.com>

<http://staffupgrade.moonfruit.com/> Today Pane ^

# What on this email can be trusted?

From "Fletcher, Freya" <ffletcher@conejouso.org> ☆

Subject **FW: ITS Administrative Support** 7:54 AM

To undisclosed-recipients; ☆ Other Actions ▾

---

**From:** Fletcher, Freya  
**Sent:** Thursday, March 05, 2015 4:47 AM  
**Subject:** ITS Administrative Support

Dear User,

Your password will expire within 24hrs Click on: [Staff & faculty update](#) to validate your e-mail.

This email has been scanned by the Symantec Email Security.cloud service.  
For more information please visit <http://www.symanteccloud.com>

<http://staffupgrade.moonfruit.com/> Today Pane ^

The actual URL is the only one of the three generated by the local computer and not the attacker.

# Problem: Private detectives

---

- People call into the main phone line claiming to be a relative and ask for information about their relation
- However, some “relatives” are really private detectives or reporters
- How might you train the phone staff to not fall for these phishing attempts?

# Authentication

# Authentication factors

---

- Something you **know**
  - Password, mother's maiden name, your address
- Something you **have**
  - Student ID card, credit card chip, RSA key
- Something you **are**
  - Finger prints, voice tones, iris, typing patterns