Security and Dependability @ VU
The People

Andrew Tanenbaum

Herbert Bos

Willem De Bruijn

Jorrit Herder

Asia Slowinska

Philip Homburg

Georgios Portokalidis
Focus

- Build a *reliable* OS
- Detect and fingerprint attacks
- Mobile devices security

Minix-3
Argos
Prospector etc
Smartphones
Minix-3

- Derives from Minix, but completely rewritten
- Deliberately small and simple
  - Kernel <4000 lines of code
- Provides
  - Stringent fault isolation
  - Stability
  - Security
- Do not compromise reliability for performance
- A lot of interest from embedded systems community
Attacks Detection @ Host

- **Argos**: honeypots
- Secure emulator employing dynamic taint analysis
- >2800 downloads
- Easily extensible
- Supported by Sentinels and NoAH

- **Eudaemon**: apply same protection to production machines

- **Prospector**: generate reliable signatures
Shelia: a client side honeypot
- Actively look for malicious server
- By going through spam folder
- Follow every link, open every attachment
- Supported by NoAH and WOMBAT
Detect Attacks - Network

- Cardguard: intrusion detection on a network card
Network Monitoring: Streamline

- Framework for high-speed I/O
- Used in several monitoring projects
Smartphones - Accessing The Internet in the Future
Smartphones – Miniature PCs

- Many applications
- Used for transactions ($)
- Privacy sensitive data
- Full blown OS + software stack implementations
Monocultures face huge dangers

Are we ready for the next killer app/phone?
( android, iphone, facebook app)
Smartphones Go Everywhere

HOME

Privacy?

ROAD

Threats?

OFFICE

By pass security?
Smartphones - Not PCs

- Limited resources
  - RAM
  - CPU
  - Battery
- Ultra-mobile
- Architecture differences
- Face more dangers from physical environment
Smartphones – Some thoughts

Things we would like to have:
- Solid security
- Data recovery
- Data privacy

Things we can’t have:
- High CPU & RAM utilisation
- Bulky transmissions
- Time consuming calculations
Smartphones: A Solution

Record → Duplicate → Always on servers
Smartphones – Many Problems

- High transmission costs (3G, WiFi)
- Bluetooth (P2P like communications)
- Detection lag (Bad guys need little time to invade privacy)
- Encryption & compression (High computation costs)
Rewind?