

# ICT in Financial Management

Topic: Security, Threats and Vulnerability

Presentation by:

Festus Kitui

[Kituif@gmail.com](mailto:Kituif@gmail.com)

+254-722-53-69-84

21<sup>st</sup> April 2017

# IT Security: Threats, Vulnerabilities and Countermeasures

# New Cyber Security World



New threats

New tools  
and services  
to protect

New  
organization  
to manage

# Cyber Crime



It is well-organized

It is advanced  
technically

It is well-financed

It has adopted a new  
view

- The old view: quick entry and exit
- The new view: hidden long term presence
- The best attack is undetected, and undetectable

# Why the Increase In Cyber Intelligence

- Recent open source network compromises disclosure, becoming more common, used as a nation enabler
- Easier to steal digits, than to integrate a spy
- Larger ROI in stealing R&D, vice actually doing it. (Past events have shown that .EDU has been used as a gateway to .GOV)

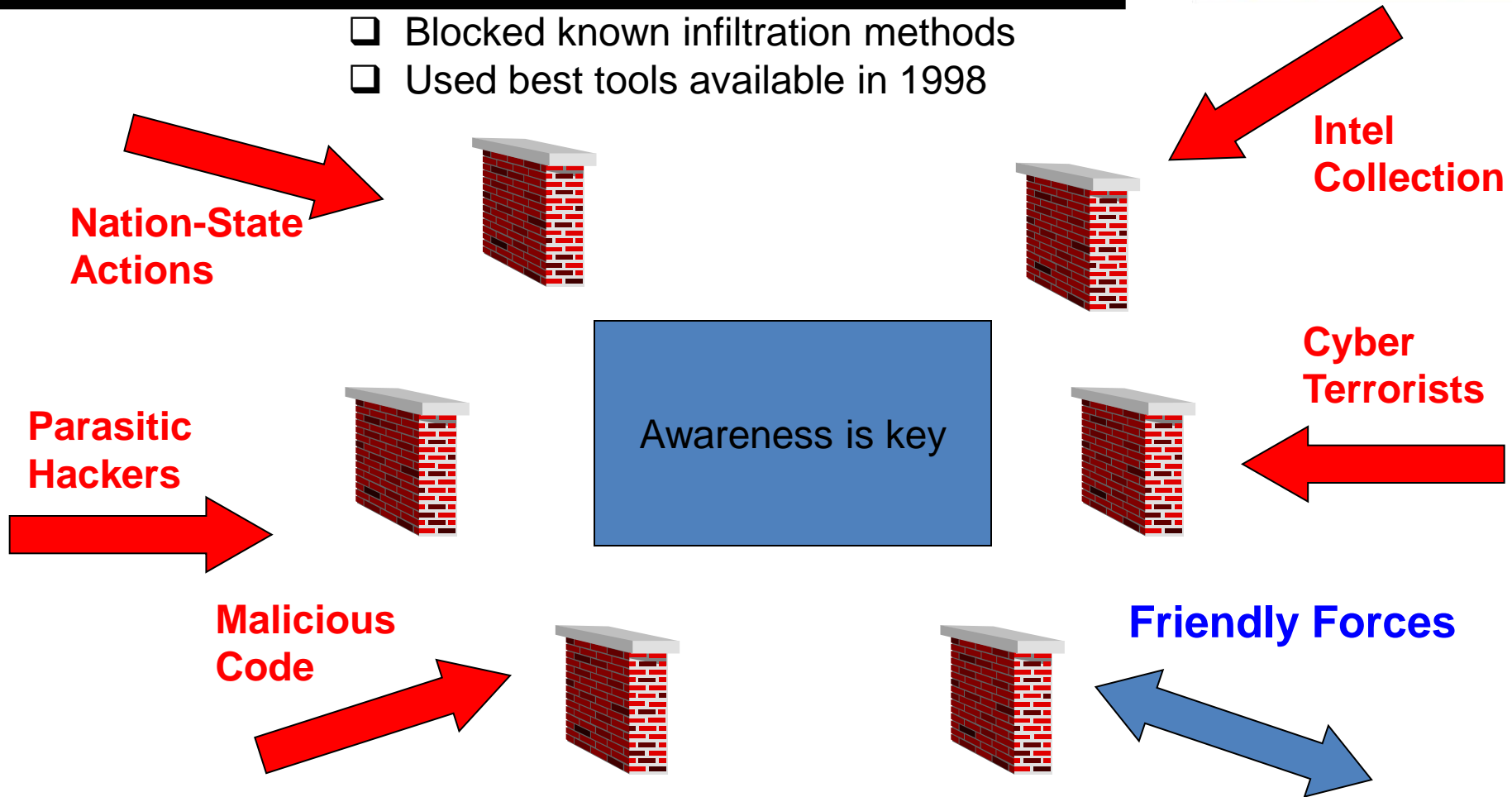


- Economic motivation
- Globalization empowerment
- Continuous national interest into US directions and intentions
- If you can't out shoot them out spend them. (costly to recover from breaches)

# Previous Defense Strategy



- ☐ Blocked known infiltration methods
- ☐ Used best tools available in 1998





## Other Vulnerabilities



- Code Mistakes
- Untrained Users
- Insecure Configuration Settings

# Code Mistakes



- Implement Prevention in Code
- Thoroughly Test
- Use Tools

# Untrained Users



- Security ignorance compromises data
- Provide the training
- Rules of Behavior
- Annual refresher training

# Insecure Configuration Settings



- Builds
- System Upgrades
- Vulnerability Scans

# Items of Special Interest



- Keyloggers
  - What are these threats and why are they of Special Interest
  - What can be done to mitigate these threats?

# Item of Special Interest: Keyloggers



- What's a Keylogger and how does it exploit a Web Application?
  - Downloaded unknowingly
  - Resident on Personal Computers
  - Captures User Activity
  - Usually part of a malicious Network

# Keylogger Mitigations



- Train users
- Implement effective Anti-Spyware, Anti-Virus
- Keep patches and versions current
- Firewall / Automatic form filler programs
- Cut and paste
- One-time passwords - OTP
- Smartcards
- **Virtual keyboards**

# Virtual Keyboard



[Forgot Password](#)

[Change Password](#)

[Edit My Account](#)

[Registration Help Files](#)

## Login to Application

UserID:

Password:



The virtual keyboard can be used in conjunction with your keyboard. The value of the key will be entered by clicking on a key or when the cursor is over the key for 2 seconds.



# Virtual Keyboard



- **Some of the features of Virtual Keyboard Include:**
  - Highly effective in evading true “Key Logging”
  - Widely used by many financial institutions
  - Does not require any new hardware or software on client machines
  - Can work in conjunction with the existing keyboard
  - Keys can be entered by mouse click or by leaving mouse on the key for 2 seconds
  - Virtual keyboard randomly shifts on the screen