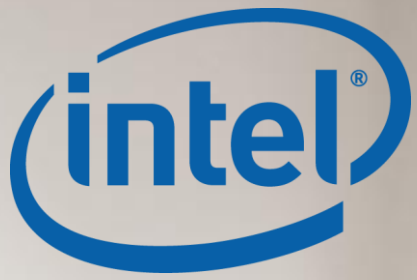
Get Rich or Get Thin: The Secure Client

Jeff Moriarty, CISSP
Security Program Manager
Intel Information Risk and Security

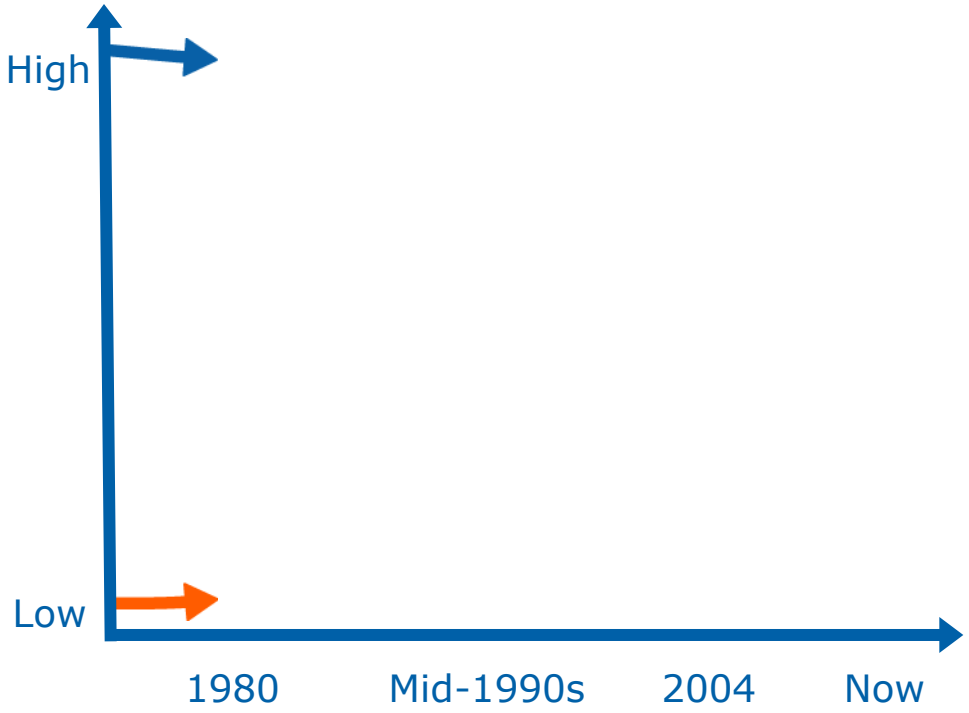


Intel - Public

Agenda

- Evolution of Attacks
- No Easy Answers
- Parity
- Rich Client Model
- Thin Client Model
- SFF Model
- SAAS & Virtualization
- Actions You Can Take

Evolution of Attacks



- Required Attacker Knowledge
- Maximum Attack Severity

Simple Attacks
Basic contagion, replicates to others, password guessing, back doors

1st Generation Attacks

Motive: Prestige, notoriety
Target: Specific systems
Impact: Cosmetic, noisy
Future: Denial of service, virus sophistication

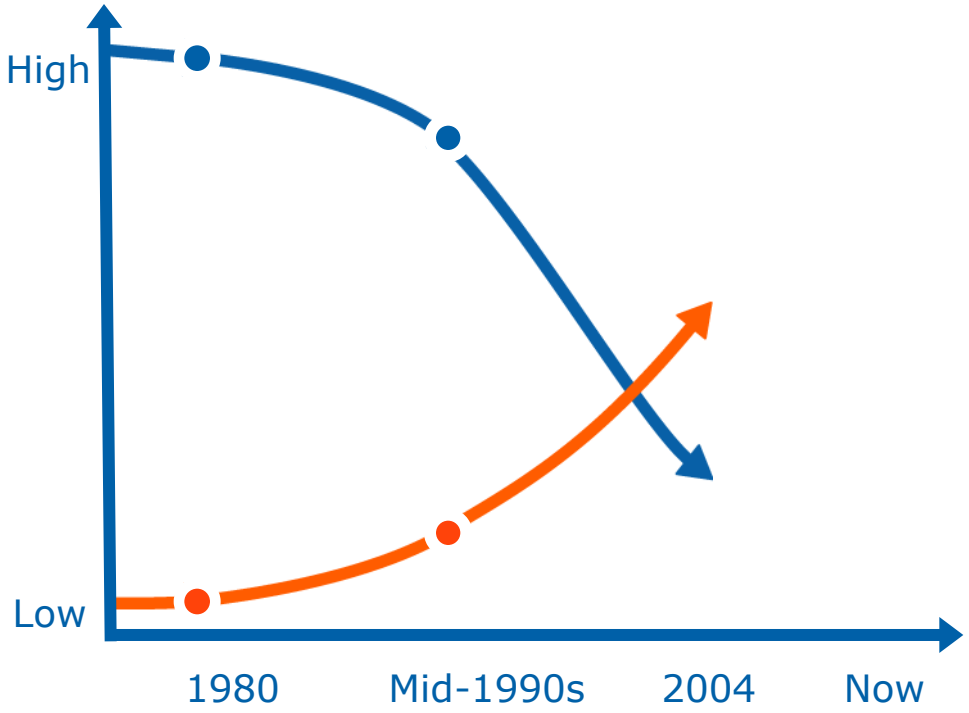
2nd Generation Attacks

Motive: Financial
Target: Compute availability
Impact: Subtle, serious
Future: Rootkits, destructive code, zero day exploits

3rd Generation Attacks

Motive: Financial, political
Target: Data
Impact: Widespread disruption
Future: Next-generation rootkits [BIOS, firmware], small form factor (SFF) malware

Evolution of Attacks



DOS, DDOS, stealth technology,
Code Red worm, SQL Slammer worm

1st Generation Attacks

Motive: Prestige, notoriety
Target: Specific systems
Impact: Cosmetic, noisy
Future: Denial of service, virus sophistication

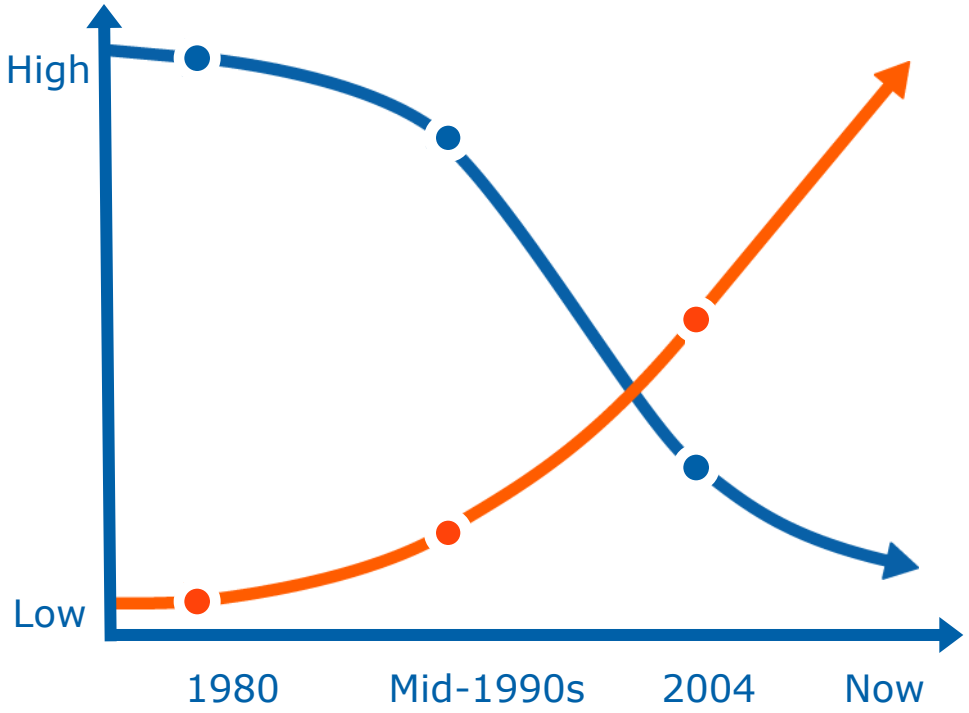
2nd Generation Attacks

Motive: Financial
Target: Compute availability
Impact: Subtle, serious
Future: Rootkits, destructive code, zero day exploits

3rd Generation Attacks

Motive: Financial, political
Target: Data
Impact: Widespread disruption
Future: Next-generation rootkits [BIOS, firmware], small form factor (SFF) malware

Evolution of Attacks



Multiple attack vectors, social engineering, stealth, active payload, zero day

1st Generation Attacks

Motive: Prestige, notoriety
Target: Specific systems
Impact: Cosmetic, noisy
Future: Denial of service, virus sophistication

2nd Generation Attacks

Motive: Financial
Target: Compute availability
Impact: Subtle, serious
Future: Rootkits, destructive code, zero day exploits

3rd Generation Attacks

Motive: Financial, political
Target: Data
Impact: Widespread disruption
Future: Next-generation rootkits [BIOS, firmware], small form factor (SFF) malware

No Easy Answers

- Today's world is challenging
- Attacks are based on Financial Motivations
- Clients and User actions are the primary attack vector
- Legal and Regulatory Climate
  - Executive Culpability
  - Due Diligence
  - Fiduciary Responsibility

Model Parity

Thin Client

- Thin Clients are **more vulnerable to attacks on availability** due to their heavy reliance on network based services and connectivity
- Thin Clients are **less vulnerable to attacks against integrity** due to lack of local storage and software

Model Parity

Thin Client

- Thin Clients are **more vulnerable to attacks on availability** due to their heavy reliance on network based services and connectivity
- Thin Clients are **less vulnerable to attacks against integrity** due to lack of local storage and software

Rich Client

- Rich Clients are **more vulnerable to attacks against integrity** due to software installed local and available local to the device
- Rich Clients are **less vulnerable to attacks on availability** due to local storage and software availability

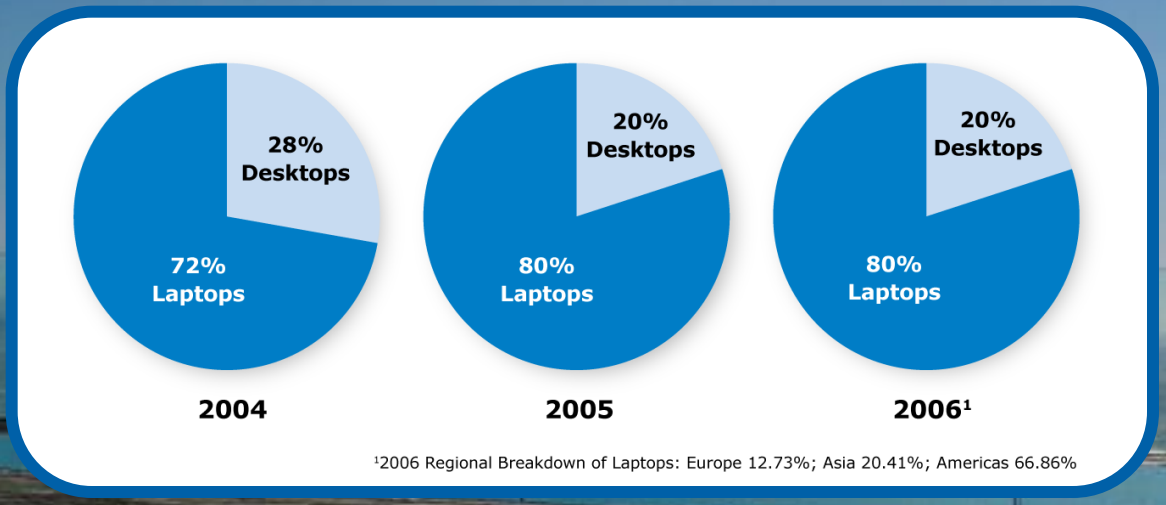
More **Client Vulnerability** Less

Rich Client Integrity

Rich Client Availability

Intel Environment Trending

- Your current client mix shows your present business model.
- Changing business models may be more costly than changing hardware purchases.



Rich Client Model

Pros

- Engineering teams and support staff are trained
- Greater availability of data
- Greater mobility
- Rich Client can mimic Thin Client, but **not** vice versa

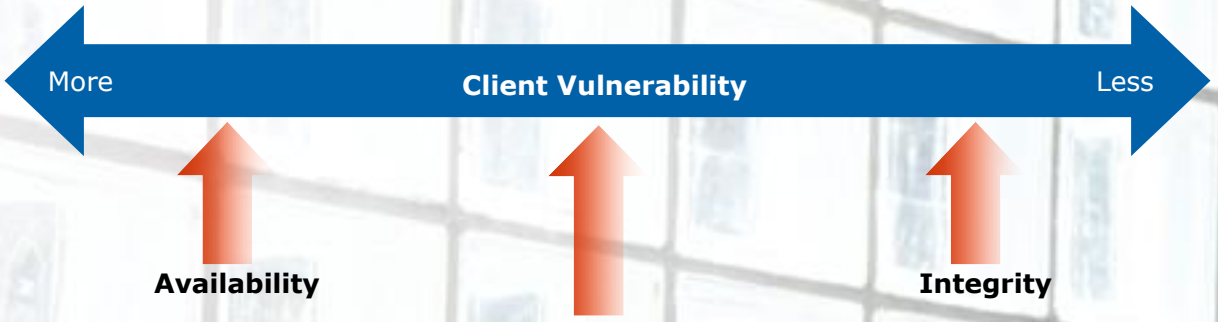
Cons

- Encrypted Data Management
- Patching
- Users

Mobility Aids Business Continuity

- Moving away from disaster
  - Employees can **take the "office" with them,** out of harm's way
- Flood hits Folsom, CA building
  - Burst water main floods office space
  - Wireless laptops **easy to relocate**
  - No customer impacts
- Snow shuts down Portland, OR
  - 5,000+ Intel employees simply **work from home** using laptops

Thin Client Model



1. **Still be comprised by hackers**
2. **End users can still fall prey to social engineering**

Pros

- Potential control of Data Leaving Network
- Potential for consolidated Security Controls
- Patching
- Prevent Users from Installing Misc Apps

Cons

- Trade Data Availability and Mobility for Security
- Single Point of Access, Single Point of Failure
  - Server **MUST** be impeccably secure
- Reduce functionality to really lock down (USB, CDROM)

Small Form Factor Model

Pros

- Hyper-mobile
- Good connectivity

Cons

- Greater theft rate
- Carrier access to data
- Potential attack vector into corporate network
- Applications not fully supported
- Attacks are ramping very rapidly compared to other models
  - Security is trailing functionality

SAAS and Virtualization

- **Software As A Service (SAAS)**
  - Both models can benefit from SAAS
  - Provides the some of the benefits of a Thin Client solution to Rich Clients

- **Virtualization**
  - OS Virtualization (Software and Hardware)
  - Application Virtualization
  - Application Wrapping

Take Action!

- **Document** Usage Models
- **Evaluate** threat/vulnerability vectors
  - Don't believe the hype…
    do your own due diligence
- **Conduct** Internal War Games
- **Prioritize** Risks and Needs

Access More IT Best Practices Resources

- Exclusive content for senior IT managers and executives in organizations with more than 100 employees
- Local seminars, webinars, podcasts, presentations, articles, white papers and more
- Optional Intel Premier IT magazine and best practices eNewsletter
- Join today at ipip.intel.com with Priority Code 482


intel
Leap ahead™


intel