

## ECE 1724: Lecture 2 – Industry Perspectives

Richard Reiner & David Lie  
Department of Electrical and Computer Engineering  
University of Toronto

1

## Industry Perspectives on Security

- Industry segmentation is complex and untidy – many partially overlapping industry sectors:
  - Personnel security
  - National security
  - Physical security
  - Homeland security
  - Public safety and security
  - Communications security
  - Aviation / transportation security
  - IT security
- We will focus on the IT Security sector only
  - Estimates vary, but approximately a \$50B global market



2

## IT Security Industry

- Alternative taxonomies of the industry:
  - People / Process / Technology
  - Network / Endpoint / Application / Messaging / Database / Data
  - Consumer / Enterprise
  - Policy definition / Policy enforcement / Compliance monitoring / Measurement
- This lecture will try to give a basic overview of what the industry is producing, and what customers are buying / deploying
- We will try to cover most these perspectives simultaneously
- Only basic detail here on each product category
  - We will go into some of these in much greater depth later in the course
- General focus on enterprise rather than consumer solutions



3

## People

- Identity and Access Management (IAM)
  - Identity Management (IDM)
    - Provisioning & de-provisioning
    - Enterprise directory
  - Access Management
    - Single sign-on (SSO): Enterprise SSO, Web SSO
    - Strong authentication
      - Tokens (hard and soft), Certificates / PKI, Smartcards
  - Authorization Management (privilege management)
    - SAML
    - Proxy solutions, native solutions, attempts at abstraction layers
  - Audit
    - Enduser and admin activities
    - Provisioning, access, action
- Training and Awareness



4

## Process

- Risk management
  - Risk modeling tools
  - Actuarial computations
- Policy & compliance framework development
  - Framework modeling tools
- Business continuity & DR
- Incident & threat management
  - Incident response platforms
- Information asset management
  - Asset inventory
- Systems development
  - Architecture
  - Modeling tools
  - Secure software development: coding standards
- Operations management
  - Availability monitoring tools



5

## Technology

- Network
- Endpoints (Servers & Desktops)
- Applications
- Database
- Messaging
- Data



6

## Technology: Network Security (1)

- Firewalls
  - Objective: partition the network into different zones / levels of trust
    - Basic: inside vs. outside (Internet)
    - More complex example:
      - Financial systems vs. less-critical servers vs. desktop segment vs. DMZ-1 vs. DMZ-2 vs. Internet
  - Types:
    - Stateless packet filters (rare, considered obsolete)
    - NAT (not designed as a security technology, but has useful “diode” properties)
    - Stateful packet filters
    - Stateful packet filters with multi-layer inspection
    - Application proxies
    - Layer-2 (bridge) vs. Layer-3 (router)
    - Anti-virus & anti-malware
  - Nearly every current product is a hybrid incorporating most of these technologies



7

## Technology: Network Security (2)

- Network Intrusion Detection and Prevention Systems (NIDS & NIPS)
  - NIDS: detect attacks on the network
  - NIPS: block attacks on the network
  - Types:
    - Signature-based: detect known attacks
    - Anomaly detection: detect statistical anomalies in aggregate traffic
    - Behavioural: detect specific events unusual at the time/place
  - Problems:
    - False positives: too many alerts (IDS) or broken network communications (IPS)
    - False negatives (attacks get through unnoticed)



8

## Technology: Network Security (3)

- Wireless (WLAN) NIDS & NIPS
  - Focus on Layer-1 and Layer-2 attacks
    - Rogue APs
    - Forced dis-association
    - Detection of un-encrypted traffic
    - Detection of WEP cracking



9

## Technology: Network Security (4)

- VPN
  - IPSec
  - SSL-VPN
  - Other non-standard technologies



10

## Technology: Network Security (5)

- Network Access Control (NAC)
  - Objectives:
    - Isolate infected or non-compliant endpoints from network assets
    - Mitigate zero-day attacks
    - Provide additional enforcement point for IAM
  - Audit capabilities:
    - OS version and patchlevel
    - Application software OS and patchlevel
    - OS security configuration / hardening
    - Application security configuration / hardening
    - Presence and enablement of security agents (AV, AM, HIDS/HIPS, ...)
  - Types:
    - Pre-admission vs. post-admission
    - Agent vs. agentless
    - Inline vs. OOB
  - Other capabilities:
    - Quarantine & Remediation



11

## Technology: Network Security (6)

- Content Security
  - Objectives: control the flow of content in and out of the organization
  - Technologies:
    - Web filtering: Prevent access to forbidden external resources (e.g. web sites)
    - Extrusion prevention / data leak prevention (DLP) / information leak prevention (ILP): prevent specified content from exiting the organization
      - Email
        - Body & attachments
      - IM
      - VoIP (low effectiveness)



12

## Technology: Network Security (7)

- Traffic shaping / QoS
  - Objectives: control data flow volumes
  - A key issue availability issue for service providers: P2P (especially BitTorrent) traffic
- Technologies:
  - Traffic classification:
    - Per-User quotas (including support for multiple classes of users)
    - Per-Protocol
      - Challenge: opaque data streams
  - Time-based
  - Progressive degradation of service with usage



13

## Technology: Endpoint Security (1)

- Anti-virus / anti-malware
  - Objective: Detect & block worms, viruses, spyware, other malware
  - Types:
    - On-demand vs. continuous scan
    - Signature-based vs. behavioural heuristics vs. sandbox emulation
    - Repair / delete / quarantine
  - Enterprise-level capabilities:
    - Outbreak management & alerting
    - Provisioning
    - Reporting
  - Historically AV and AM were separate product categories, but they have largely converged
  - Nearly every current product is a hybrid incorporating most of these technologies



14

## Technology: Endpoint Security (2)

- Endpoint (Host) Firewall
  - Objective: protect the endpoint from potentially hostile network traffic
  - Types:
    - Packet filters (stateful)
    - Application proxies
    - Local software privilege management
  - Nearly every current product is a hybrid incorporating most of these technologies



15

## Technology: Endpoint Security (3)

- Host IDS / IPS (HIDS / HIPS)
  - Objective: protect the endpoint from network-borne attacks
  - Types:
    - Signature-based: detect known attacks
    - Anomaly detection: detect statistical anomalies in aggregate traffic
    - Behavioural: detect specific events unusual at the time/place
    - Local software privilege management
  - Nearly every current product is a hybrid incorporating most of these technologies



16

## Technology: Endpoint Security (4)

- Endpoint configuration management
  - Audit capabilities:
    - OS version and patchlevel
    - Application software OS and patchlevel
    - OS security configuration / hardening
    - Application security configuration / hardening
    - Presence and enablement of security agents (AV, AM, HIDS/HIPS, ...)
  - Audit software inventory
    - All required components present
    - No forbidden components present



17

## Technology: Application Security (1)

- Static Analysis Tools
  - Objective: inspect applications to detect vulnerabilities
  - Types:
    - Source code inspection
    - Object code inspection (generally requires a build with debug symbols, although the DoD-sponsored KDM effort seems to be able to produce good results without)
    - Products specialized by language & platform (Java, C# on .NET, C/C++, Windows, Linux, ...)
  - Limitation: generally cannot see vulnerabilities inherited from shared libraries / DLLs, or from third-party frameworks and toolkits



18

## Technology: Application Security (2)

- Web Application Firewalls
  - Objective: Protect web-based application against applicable attacks (SQL injection, XSS, etc.)
  - Types:
    - Inline vs OOB
    - Whitelist vs. blacklist
      - Whitelist: learning or discovery vs. authoring (also guided-authoring tools)
      - Blacklist often not very effective



19

## Technology: Application Security (3)

- XML Firewalls
  - Objective: Protect XML-based systems (e.g. SOAP web-services)
  - Risks include DoS against XML parsers
  - Other capabilities include validation (XML schema or other), signature verification, content scanning



20

## Technology: Messaging Security (1)

- Anti-Virus and Anti-Malware products specialized for email and IM traffic
  - Problems:
    - Encrypted attachments
    - Unknown file formats



21

## Technology: Messaging Security (2)

- Anti-SPAM (for email and IM)
  - Technologies:
    - Blacklisting of sending sites: DNSBLs
      - Address and MX honeypots to populate BLs
    - Greylisting (temporary rejection)
    - Whitelisting
    - Challenge-Response (per sender/receiver pair)
    - Distributed message checksum catalogues
    - NOOP MX servers at top of priority list
    - PTR/Reverse DNS checking
    - Rule-based content filtering
    - Bayesian filtering
    - SMTP callback verification
    - Sender authentication (SPF, DomainKeys)
  - Nearly every current product is a hybrid incorporating most of these technologies



22

## Technology: Messaging Security (3)

- Email encryption
  - Objective: confidentiality and integrity of email messages
  - Standards:
    - S/MIME
    - PGP, PGP/MIME
  - Challenge: key management
  - Implementations:
    - Endpoint
      - High user complexity
    - Gateway
      - Poor differential control over access to keys, often can offer organizational proof only rather than user-level proof



23

## Technology: Database Security

- Database encryption
  - Table-, column-, or row-level
  - Key management is again the challenge
- Database monitoring
  - Special case of HIDS/HIPS (see above)
- Database security assessment
  - Special case of VA tools (see above)



24

## Technology: Data Security

- Disk and file encryption
  - Objective: protect stored data (confidentiality and integrity)
- Risks:
  - Physical loss (laptop)
    - Leading to unauthorized access
  - Intrusion (desktop / server)
    - Leading to unauthorized access
    - Leading to data integrity problems
- Technologies
  - OS components / addons
  - Hardware (disk)
- Challenges
  - As usual, key management is the hard part



25

## Technology: Data Security

- Digital Rights Management
  - Objective: control permitted use / distribution of data files
    - Music or video
    - Sensitive enterprise documents
  - Always crypto-based
  - Challenge is again key management and how to make that invisible to a broad set of endusers



26

## Technology: Security Management

- Security Information Management (SIM) / Security Event Management (SEM) / Security Information and Event Management (SIEM)
  - Objective: consolidate and correlate security data
    - Security events (alerts)
      - FW, NIDS/NIPS, HIDS/HIPS, AV, AS, NAC, WAF, etc.
    - VA scan results
    - Data traffic (NetFlow etc.)
    - IDM
      - Provisioning events
      - Authentication events
      - Authorization events



27