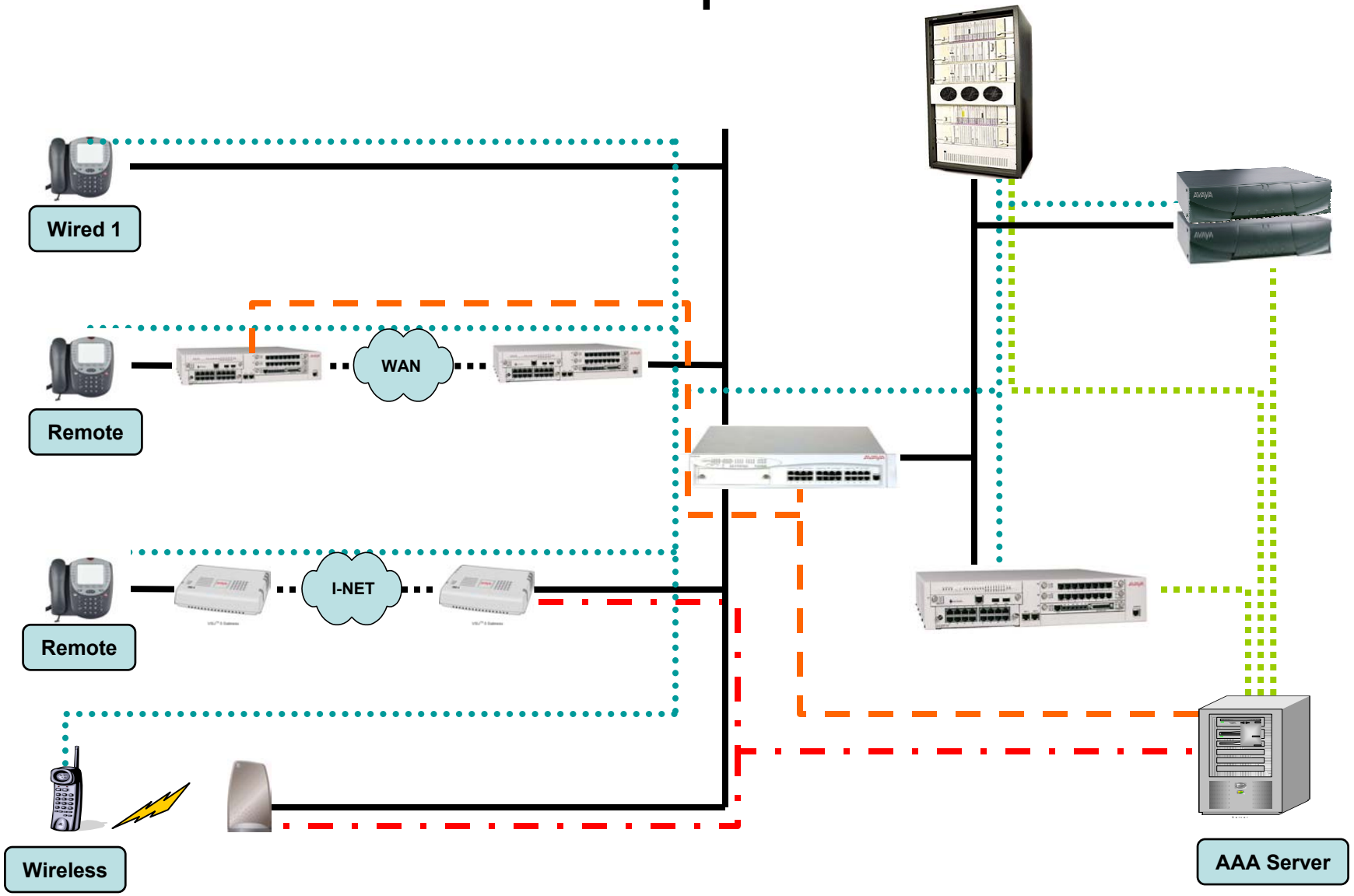
Link Security Considerations in the Enterprise

Mahalingam Mani

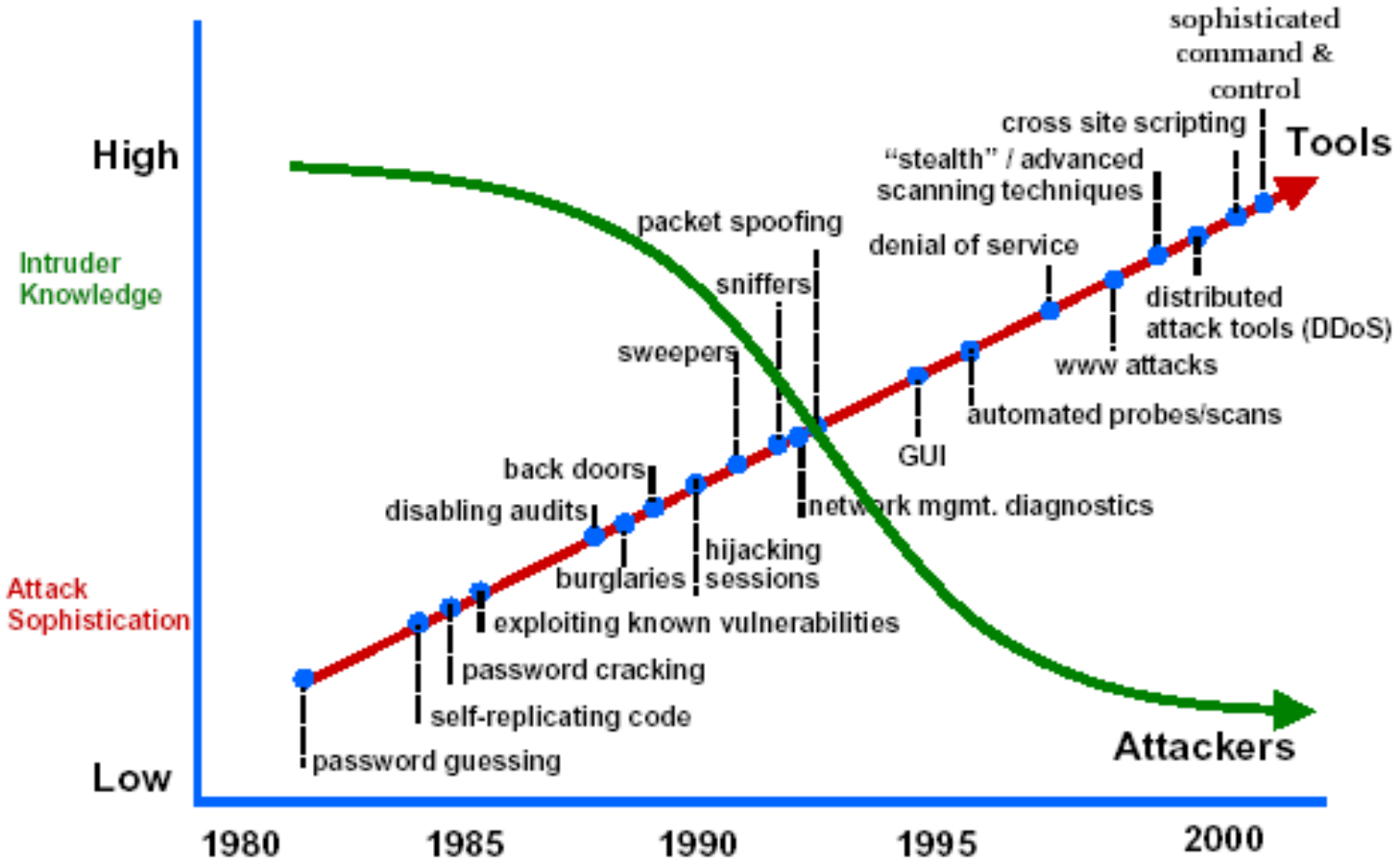
Enterprise Security in Brief

- **Point Security**
  - **System Protection: beyond standards**
    - **Servers upto application level**
    - **Layer 2 & 3 Network Devices**
  - **Perimeter Protection**
    - **Infrastructure Perimeter: firewalls, etc.**
    - **Extended Perimeter (of remote access)**
  - **Link layer protection**
    - **Predominantly confined to weak MAC level access control and now to some extent 802.1X**
- **Path Security**
  - **Upper layer (IP, application) protection of communication protocols**
    - **IPsec tunnel/transport modes; TLS transport layer, ...**
    - **Routing protocol security**
  - **Link-layer**
    - **Largely confined to port, MAC based access control**
    - **Network segmentation by use of VLAN's.**

An Enterprise View

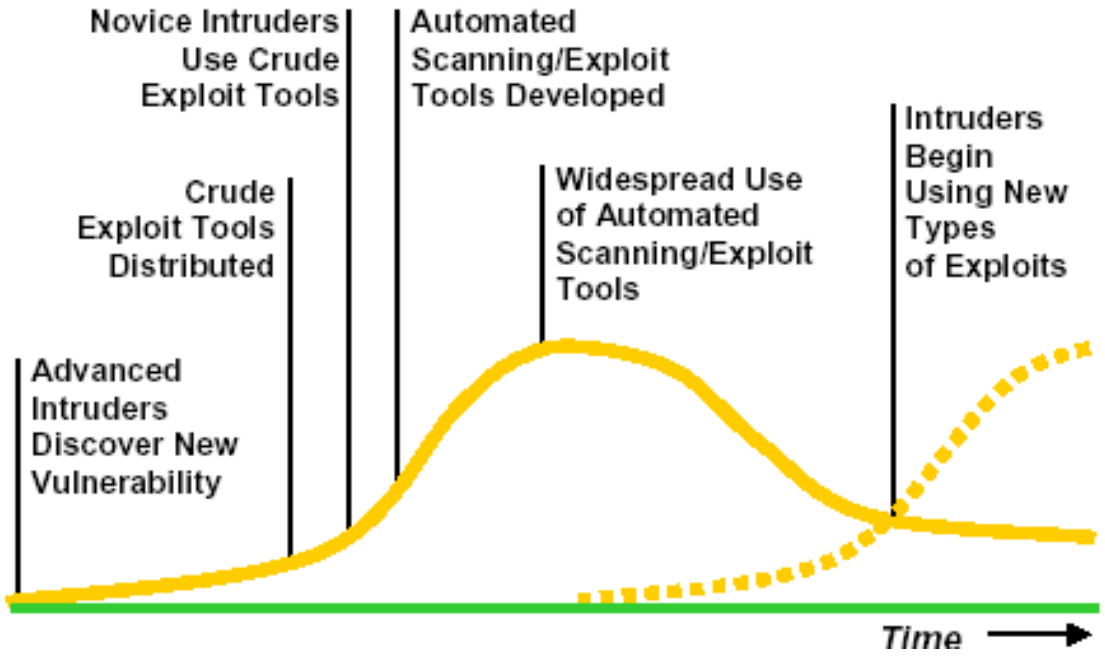


Attack trends: sophistication vs. knowledge



Source: CERT

Vulnerability Exploit Cycle.



Patch-n-Pray will not be enough in the long run.

Source: CERT

Enterprise Threat Model.

- **Internal breaches account for >70% of all attacks.**
  - Well published fact
  - Attacks on communication protocols comparable to system exploits
  - As IP and higher layer threats are addressed, lower layer threats are bound to become the focus.
- Link Layer Threat of unauthorized bridges
  - Modification of
    - MAC layer control & management traffic
    - Link Layer Protocols: Spanning Tree, Rapid STP,…
    - modification of addresses, identity spoofing and hijacking.
  - Unauthorized disclosure of data.
- **Trust of network dependent on & includes trust of bridges along the path.**

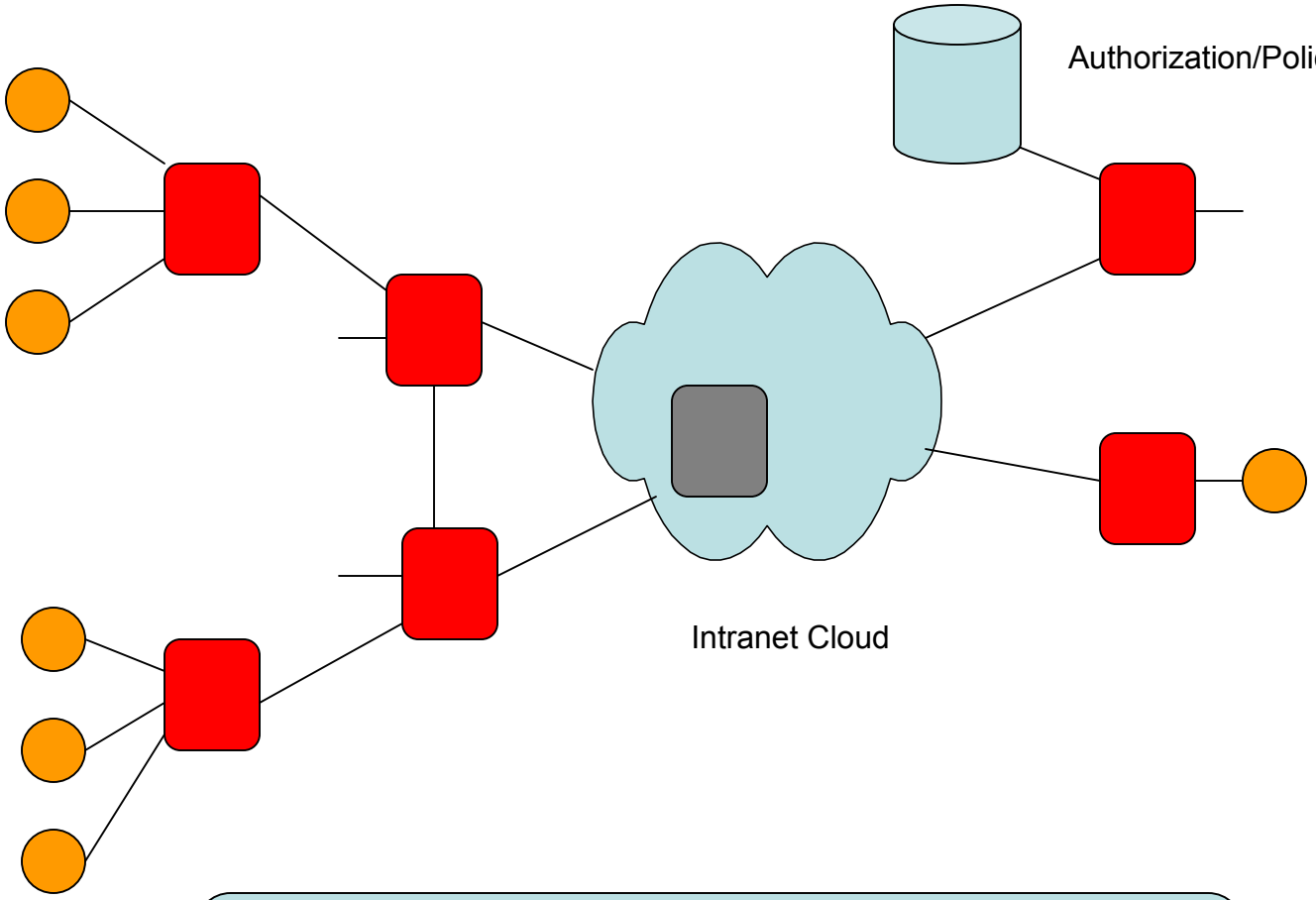
Threat Detection or Protection?

- Enterprises have the advantage of tighter network administration and monitoring.
- Endpoints depend on trusting the bridges
- Bridges in network need a mutual mesh of trust.
- Is it sufficient to detect possible attacks on bridges
  - Leaving link layer data protection unnecessary?
- Can authorization framework be separated from authentication sequence?
- How important is protection of bridge protocols over datapath?
- Where's the bootstrapping of trust when control/management frames have to be protected?

A Link Security Trust Model

- Link Layer is the backbone to enterprise connectivity
- A two-tiered trust model is proposed.
  - Endpoints trust a near-neighbor
  - Bridges weave a mesh of trust.
- Bridge is the unit of node security: security enforcement point
- Trust Anchor
  - The bridges shall not have link-layer dependencies to access trust anchor at runtime
  - *A priori* provisioning should allow a distributed and self-contained trust model
- Authentication
  - Based on identity of bridge bound to a cryptographic key by the trust anchor – e.g., a public-key model (or bidirectional 802.1X?)
  - Computational complexity in keeping with the device capacity.
  - Desirable: consistency, if not compatibility, with Wireless (LAN) bridges.
- Authorization
  - Endpoints (node) access control may be based on local policies/servers
  - No link-layer constraints on authorization servers.
    - Implies authorization is contingent on reach-ability of Policy server(s).
- Secure Data Exchange
  - Model compatible with 802.10
  - Include replay protection

Distributed End-end Security Model.



- **Secure bridges authenticate autonomously mutually.**
- **Endpoints authenticate to the nearest neighbor bridge(s)**
  - **Discovery of Secure Bridges**
  - **Link-layer encapsulation between SDE bridges**

Security-aware bridge

Security unaware bridge

Summary

- Distributed Authentication model preferable over discrete authentication server model
  - Revocations are an issue.
  - Optional Bidirectional Authentication for small deployments
- Centralized Policy Server for access control
- Enhanced 802.10 SDE
  - Providing support for VLAN, QoS tags
  - Replay Protection service