Time to Compromise of Networked Systems

A Dynamic Model of Attack, Defense, and Isolation in the Era of AI and Quantum Acceleration

Michael Voss

EtherGap Corporation
March 2025

Abstract

As cyber attack capabilities accelerate through artificial intelligence and emerging quantum technologies, traditional network-based defensive strategies are increasingly outpaced. This paper introduces a conceptual model for **time to compromise (tc)** as a function of attack intensity, attack complexity, defense efficacy, inherent system vulnerability, and the availability of attack paths.

We demonstrate that for continuously networked systems, tc tends to **decrease over time** due to asymmetric acceleration in offensive capabilities. However, the introduction of **true Layer 1 physical isolation** fundamentally alters this dynamic by removing entire classes of attack paths. In such systems, the expected time to compromise for remote network-based attacks approaches **infinity**, shifting the threat model from probabilistic to condition-based.

We further introduce a **dual isolation architecture**, in which connectivity between system layers is mutually exclusive in time, ensuring that no persistent path exists between protected assets and external networks. A real-world case study in power generation infrastructure is presented to illustrate these effects in practice within regulated environments.

---

1. Introduction

Modern cybersecurity is defined by an asymmetry: attackers require only one viable path to succeed, while defenders must secure all possible paths. Most defensive strategies operate within OSI Layers 2 through 7, assuming continuous physical connectivity.

This assumption introduces a structural vulnerability. As attack capabilities scale through automation, distributed infrastructure, and intelligent tooling, the effective attack surface of connected systems expands over time—even as defensive controls improve.

This paper proposes a model for **time to compromise (tc)** to formalize this dynamic and explores how architectural decisions—particularly physical isolation—affect the trajectory of system exposure.

---

2. Model Definition

We define time to compromise as a function of five primary variables:

- **Attack Intensity (AI(t))**
  The rate and volume of attack attempts over time
- **Attack Complexity (AC(t))**
  The sophistication and effectiveness of attack techniques
- **Defense Efficacy (DE(t))**
  The effectiveness of defensive measures over time
- **Inherent Vulnerability (IV)**
  Baseline susceptibility based on system design and implementation
- **Attack Path Availability (AP(t))**
  The existence and accessibility of viable paths through which an attacker can reach the system

A conceptual relationship can be expressed as:

$$tc \propto \frac{IV \cdot DE(t)}{AI(t) \cdot AC(t) \cdot AP(t)}$$

---

3. Interpretation of the Model

This formulation yields several key insights:

- Increasing **AI(t)** or **AC(t)** decreases tc
- Increasing **DE(t)** increases tc
- **IV** represents baseline exposure independent of time
- **AP(t)** acts as a gating variable for compromise

The most important implication is:

$$\text{If } AP(t) \to 0, \text{ then } tc \to \infty$$

This is not an incremental improvement in defense—it is a categorical shift. If no viable attack path exists, compromise cannot occur via that vector regardless of attack intensity or sophistication.

---

4. Technological Acceleration

Emerging technologies are accelerating attack capabilities at a rate that outpaces defensive improvements:

- **Artificial Intelligence (A)** enables automated reconnaissance, vulnerability discovery, and adaptive exploitation
- **Quantum Computing (Q)** introduces potential disruption to cryptographic protections and reduces the cost of certain attacks

We incorporate these effects as accelerants:

$$tc \propto \frac{IV \cdot DE(t) \cdot f_A^{(def)}}{AI(t) \cdot AC(t) \cdot f_A^{(att)} \cdot f_Q \cdot AP(t)}$$

Where:

- $f_A^{(att)} > f_A^{(def)}$, reflecting asymmetry in favor of attackers
- f_Q amplifies attack complexity

For continuously connected systems, these factors cause the denominator to grow over time, resulting in:

$$tc \to 0$$

meaning that compromise becomes faster and more likely as attack capabilities scale.

---

5. Continuous Connectivity and Declining tc

In traditional networked architectures:

- **AP(t)** remains persistently greater than zero
- Systems are continuously exposed to global attack activity
- Attack surfaces evolve and expand

Even with improvements in defensive controls, the effective outcome is:

A gradual reduction in time to compromise as attack intensity and complexity increase over time.

This reflects a structural limitation of connectivity-dependent security models.

---

6. Impact of Layer 1 Physical Isolation

The introduction of **true Layer 1 physical isolation** fundamentally changes the model.

Rather than attempting to mitigate attack vectors, physical isolation **removes them entirely** for remote network-based threats.

For those attack classes:

$$AP_{remote}(t) \to 0$$

Therefore:

$$tc_{remote} \to \infty$$

This means:

- Remote compromise becomes structurally infeasible rather than merely unlikely
- Increases in global attack intensity and sophistication no longer affect the system for those vectors

Security is no longer governed by probabilistic resistance to attack, but by the absence of a viable path.

---

7. Hybrid Isolation Architectures

Pure isolation can introduce operational constraints, particularly in environments requiring monitoring, maintenance, or data exchange.

Hybrid architectures address this by enabling controlled interaction while preserving isolation properties. Common techniques include:

- Out-of-band signaling channels
- Unidirectional communication mechanisms (e.g., data diodes)
- Dual isolation boundaries
- Tamper-evident logging systems

These approaches aim to maintain:

$$AP_{remote}(t) \approx 0$$

while allowing limited, controlled system interaction.

7.1 Dual Isolation Architecture (Optional Control Model)

An extension of the isolation concept is the use of **dual isolation architectures**, which enforce mutually exclusive connectivity between network domains.

In this model:

- A **protected asset** (e.g., PLC, controller, or critical system) is physically isolated
- A **local network (LAN)** serves as an intermediate domain
- The LAN may connect to a **wide-area network (WAN)** for external communication

The defining property is:

At no point does a continuous Layer 1 path exist between the protected asset and the WAN.

This is enforced such that:

- When the protected asset is connected to the LAN,
  → the LAN is simultaneously disconnected from the WAN
- When the LAN is connected to the WAN,
  → the protected asset is disconnected from the LAN

This creates a **time-segmented connectivity model** in which:

$$AP_{protected \rightarrow WAN}(t) = 0 \quad \forall t$$

Use Cases

Dual isolation is particularly applicable in environments where:

- Vendors require **private or controlled access** for maintenance
- Systems rely on **periodic, not continuous, communication**
- Regulatory frameworks encourage segmentation and controlled access

Examples include:

- Industrial maintenance windows
- Vendor access via private networks
- Data staging and supervised transfer environments

Impact on Time to Compromise

Within the model:

- The protected asset maintains:

$$AP_{remote}(t) = 0$$

with respect to WAN-originating threats

- Exposure is shifted to the intermediate LAN, which can be independently monitored and controlled
- Compromise requires:
  - exploitation during a controlled connection window, or
  - successful propagation from a compromised intermediate system

This significantly increases tc while preserving operational flexibility.

---

8. Real-World Case Study: Central California Power Generation Facilities

Context

A physically enforced Layer 1 isolation architecture was deployed in **two natural gas turbine power generation facilities in Central California** to meet NERC **Critical Infrastructure Protection (CIP)** requirements.

These facilities represent high-value targets due to their role in grid stability and their exposure to advanced persistent threats.

Architecture Characteristics

The deployed system incorporated:

- True Layer 1 physical isolation
- Out-of-band signaling for supervisory interaction
- Dual isolation boundaries
- Tamper-evident logging mechanisms

The design objective was to eliminate all routable and protocol-based attack paths while preserving operational visibility.

Observed Effects

- Elimination of remote attack surface
- Decoupling from global attack trends
- Stabilization of exposure over time
- Simplified compliance posture

Implications for Time to Compromise

Within the model:

$$AP_{remote}(t) \to 0 \quad \Rightarrow \quad tc_{remote} \to \infty$$

Compromise shifts from a probabilistic outcome driven by global attack pressure to a condition-based outcome dependent on:

- physical access
- insider threat

- procedural failure
- supply chain or maintenance pathways

---

9. Discussion

The model highlights a fundamental limitation of conventional cybersecurity approaches:

Defensive strategies that preserve attack paths remain subject to accelerating offensive pressure.

While technologies such as AI can enhance defense, they do not eliminate exposure. Only architectural decisions that remove attack paths can fundamentally alter the trajectory of time to compromise.

---

10. Conclusion

The concept of **time to compromise (tc)** provides a useful framework for evaluating cybersecurity architectures under conditions of accelerating attack capability.

For continuously connected systems:

$$tc \to 0$$

over time as attack intensity and complexity increase.

For physically isolated systems:

$$tc_{remote} \to \infty$$

for remote attack classes.

This distinction is critical:

Security is not solely a function of stronger defenses, but of whether viable attack paths exist at all.

Architectures incorporating **Layer 1 isolation, controlled interaction, and path elimination strategies** represent a structural shift from reactive defense to foundational resilience.