关于网络安全行业生态演进的思考

张矩　　斯道资本

2018 ISC 互联网安全大会 中国·北京
Internet Security Conference 2018　Beijing·China
（原中国互联网安全大会）

投资人与从业者对行业理解的视角

抽象 → 泛化 → 应用

投资人

从业者

具象 → 计划 → 执行

网络安全的基础商业逻辑

安全防护的价值通常由被保护的资产的价值决定：

- 信息安全事件的损害通常是潜性并滞后于事件发生的。
- 信息的保有者与信息安全事件中的受害者往往是不一致的。
- 强制性合规是第二类价值体现。
- 法律法规是保证信息价值得到合理评估的主要手段。

安全防护的价值悖论：

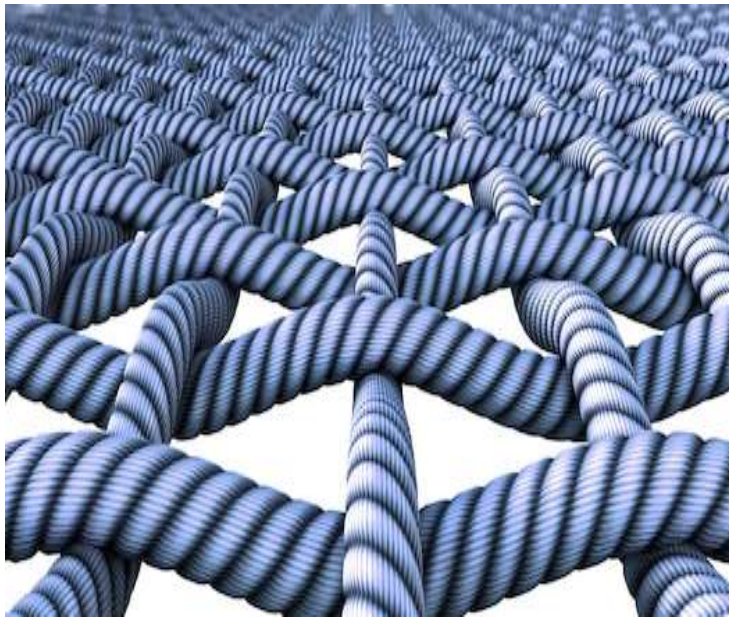
- 门锁的售价和滴滴的垄断。
- 用户对于安全产品评估能力的缺失导致劣币驱逐良币。

安全：新一代信息系统架构的基底

FABRIC：从边界到叠加到嵌入到原生

- SECURITY BY DESIGN：
  - 复杂系统的不可设计性；
  - 可定义的可用性与安全性的妥协

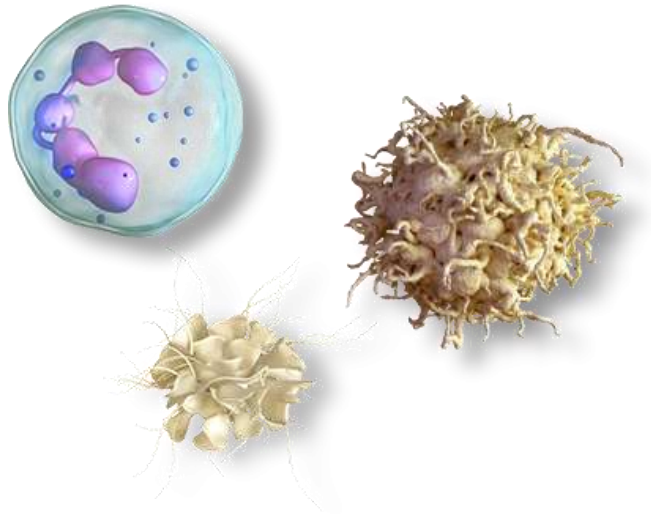
- VERIFICATION：
  - 可追溯，可验证的实现



网络安全行业生态的演进：合理化共生

在正常商业逻辑下，基于利益获取的网络安全对抗行为可通过行为成本与收益分析来理解：

- 行为理性化：安全成本线性，适度的成本获取可接受的安全
- 生态平衡化：除非重大的技术变革，对抗双方形成准平衡态持续扩大的市场
- 厂商分工化：几乎所有的厂商都是防御提供者，分工协同
- 损害隐形化，慢性化：利益获取和时间正比
- 惩罚性成本：法律是平衡成本不对称性的重要手段



网络安全行业生态的演进：非理性破坏

在非理性目标驱使下，面向造成对手最大破坏性的安全对抗行为将造成另一类网络安全生态：

- 成本非线性化：高阈值成本投入获得可接受安全水平
- 生态对抗化：技术手段高度专业化，武器化
- 厂商集中化：模糊的攻击者和防御者的界限，倾向于形成集中式垄断型厂商
- 事件黑天鹅化：影响力大不可预测的网络安全事件
- 不可惩罚性：难以溯源，难以取证，难以执法

网络安全行业生态的演进：展望

IT系统全生命周期安全化：

- 网络安全集成商和管理服务提供商崛起

面对非理性的极端对抗：

- 网络安全领域的军工共同体出现

云化，无服务器化，GDPR（及未来）：

- 服务访问安全（API安全）
- 数据流动安全（INTEGRATION安全）

ISC 2018
ISC互联网安全大会

360互联网安全中心

谢 谢！

2018 ISC 互联网安全大会 中国 · 北京

Internet Security Conference 2018 Beijing · China

（原中国互联网安全大会）