



ISC 互联网安全大会



360 互联网安全中心

技术创新无止境 创造安全新作用

谢朝霞 安络科技CEO

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



ISC 互联网安全大会



360 互联网安全中心

目录

从计算机体系结构到网络安全

网络安全需求的本质

创造安全新作用

ZERO TRUST SECURITY

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL

计算机科学的创新架构：层次化模块化(封装)



ISC 互联网安全大会



360 互联网安全中心

网络应用层

21/53/80/110/135/139/443/1433/3389... | 浏览器/邮件/App

IP/TCP/UDP/ICMP

系统应用层

网络应用程序

数据库

本地应用程序

本地服务

网络服务

桌面

操作系统、硬件驱动程序、文件驱动、网络驱动

物理层

硬盘

大规模集成电路（存储、计算、通信，如RAM，CPU，网络控制芯片）

磁头

模拟电路

数字电路

光器件

磁效应

电效应(继电器效应\触发器效应，串联/并联)

光效应

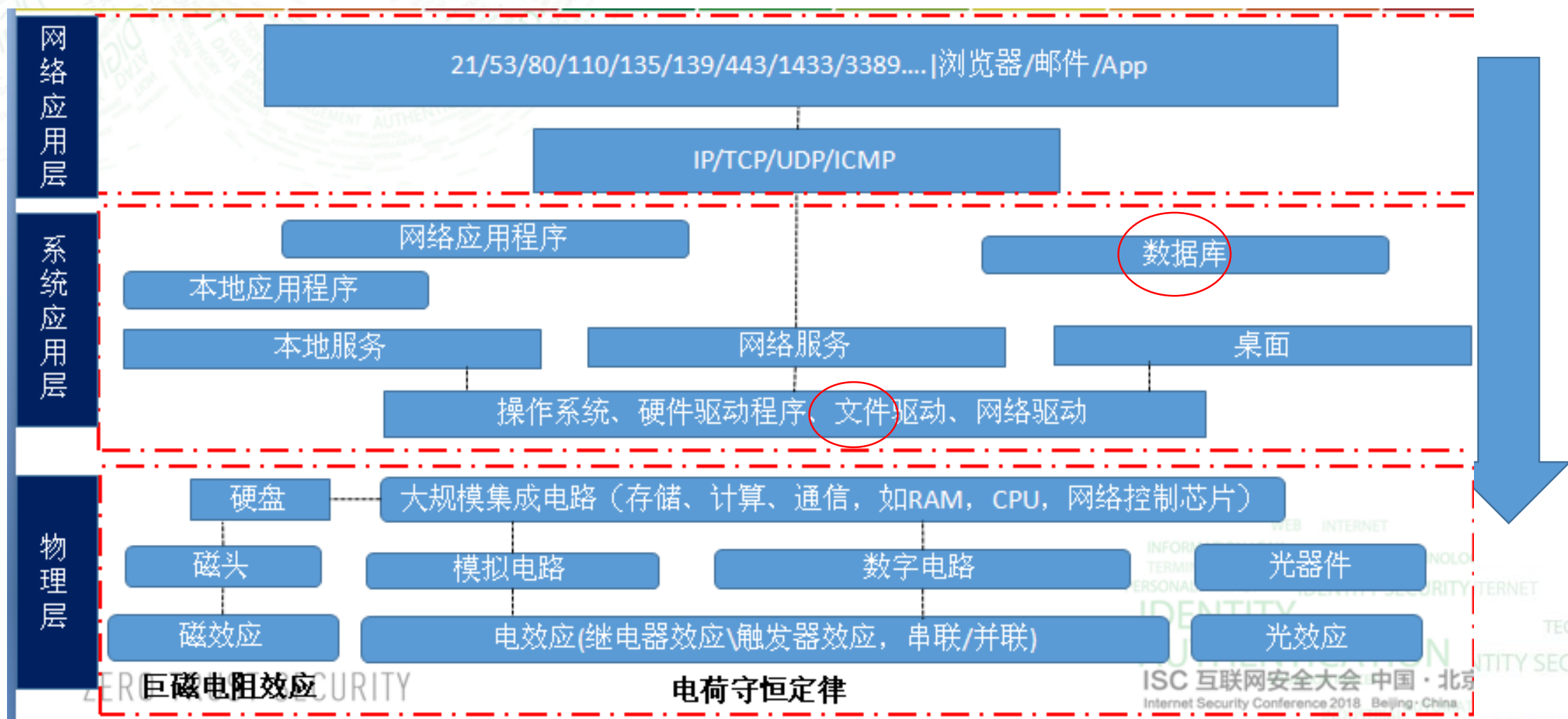
巨磁电阻效应

电荷守恒定律

组合创新：现代计算机网络电子产品



攻击者的路径依赖



需求：

斯莱沃斯基：《需求》一书中曾写到：“需求就是满足人类的物质与情感的各种需要，那些生活中产生痛苦、不便、浪费、乃至危险的麻烦、各样的不满足，组成了人们的需求。”

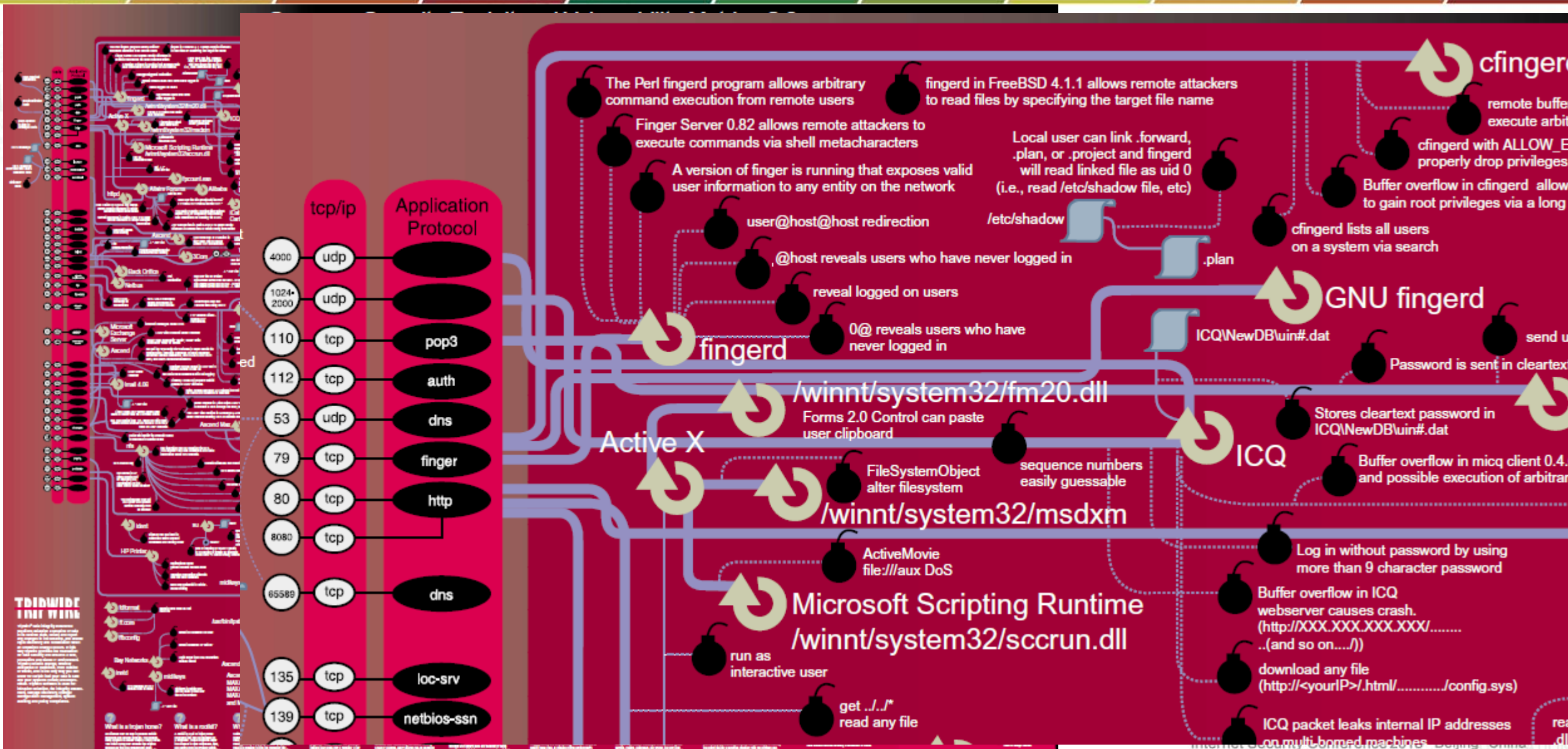
如何让老百姓不受骗？
怎样让核心技术不流失不扩散？
舆情象水，如何因势利导地利用和治理？
如何将高科技高智商犯罪分子绳之以法？

以上才是安全需求，找漏洞，打补丁，安全管理.....这些都不是。

◆ 《中华人民共和国刑法》中的469个罪名，其中有130个可以借助网络实施。

可以借助或通过网络实施的犯罪罪名		
大类	比例	备注
危害国家安全罪	10/12	除武装叛乱暴乱罪、叛逃罪外
危害公共安全罪	5/52	如破坏电力设备罪、帮助恐怖活动罪、宣扬恐怖主义罪
破坏社会主义市场经济秩序罪	59/108	包括销售伪劣商品罪、破坏金融管理秩序罪（如洗钱罪、非法吸收公众存款罪）、金融诈骗罪（如集资诈骗罪）、扰乱市场秩序罪（如组织领导传销活动罪）
侵犯公民人身权利、民主权利罪	7/42	如侵犯公民个人信息罪、侮辱罪、诽谤罪
侵犯财产罪	4/13	如盗窃罪、诈骗罪、敲诈勒索罪
妨害社会管理秩序罪	41/138	如非法侵入计算机信息系统罪、非法利用信息网络罪、寻衅滋事罪
危害国防利益罪	4/23	如伪造变造买卖武装部队公文证件印章罪

传统网络攻防的视线范围



攻防四象限/防守方的规则法律困境

隐藏/伪装/检查

进攻方的防守

防守方的防守

我们过去
只关心一、
三象限

进攻方的进攻

防守方的进攻

战场前移：
技术战/心理
战/法律战

ZERO TRUST SECURITY

攻防元素周期表



进攻端元素					中性元素	防守端元素				
Dc 解密									Ec 加密	
Ck 密码破解	Oa 溢出攻击						Sk 密钥	Sp SSL协议	Dp 动态密码	
Da 反汇编	As ARP欺骗	Sf 嗅探	Fz fuzzing	Rk rootkit	关联分析	Vs Virusscan	Ac 访问控制	Pd 包检测	Pf 包过滤	
Sc 扫描	Hj 劫持	Df DNS欺骗	Si Script注入	Ma 中间人	数据碰撞	La 日志审计	Bl 黑名单	Wl 白名单	Vs 漏洞扫描	
Ca 跨站	Nf 网络钓鱼	Mb Mailbomb	Hd HashDump	Ra 路由攻击	数据分析	Ta 流量分析	Ds 数字签名	Dr 数据恢复	Db 数据备份	
Ba 旁路	Rp 重放	Fa D.o.S	Rb 彩虹表	Hp 鱼叉攻击	信息搜集	Id IDS	Pk PKI	Vp VPN	Vm 虚拟机	
Ep 本地提权	Ne 网络提权	Lc Impression clean	Wh 水坑攻击	Wc Wifi破解	社会工程	Ip IPS	Fw 防火墙	Ta 终端管理	Wf WAF	

ZERO

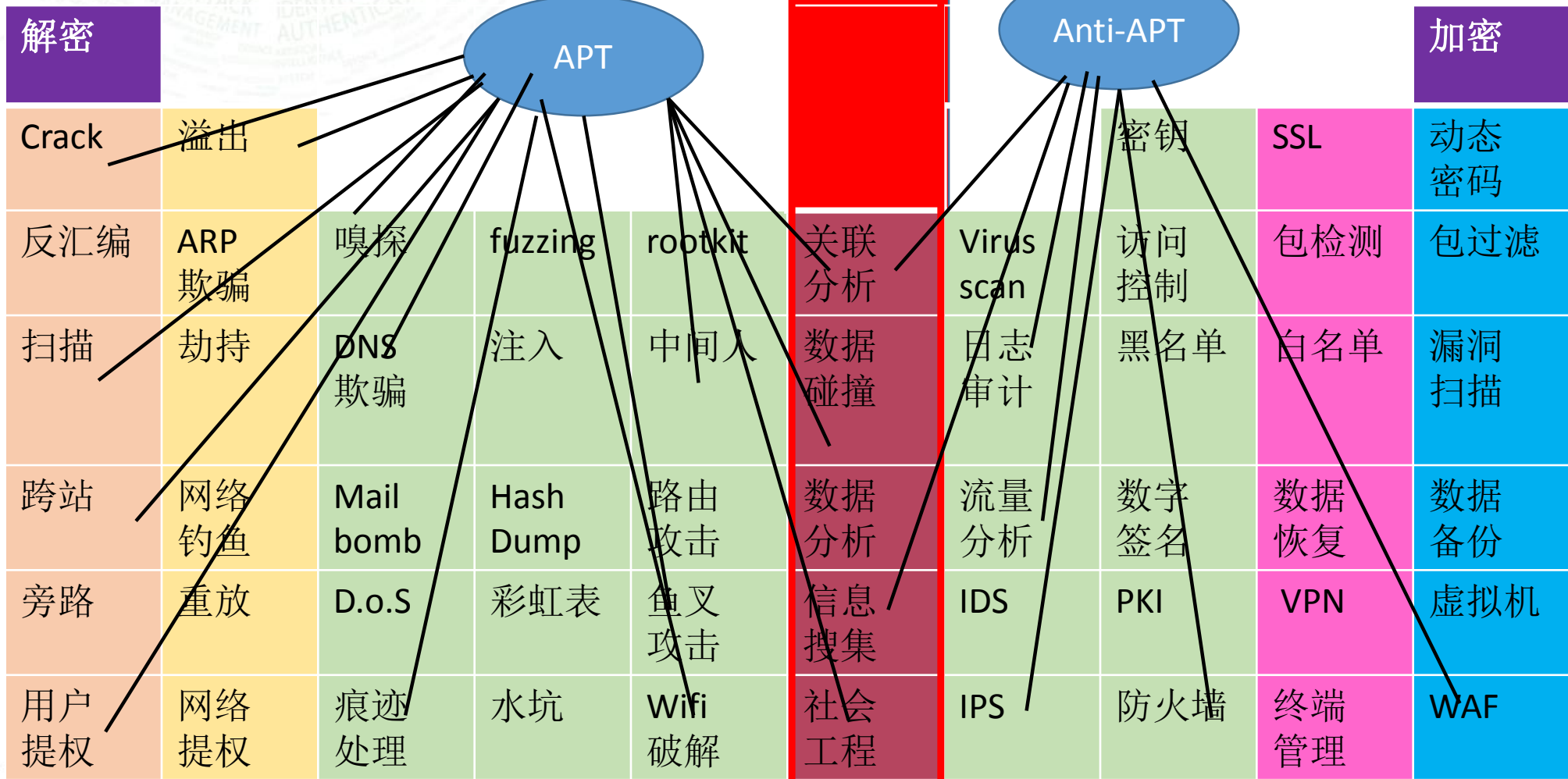
攻防两端元素组合样例



进攻端元素

交叉元素

防守端元素



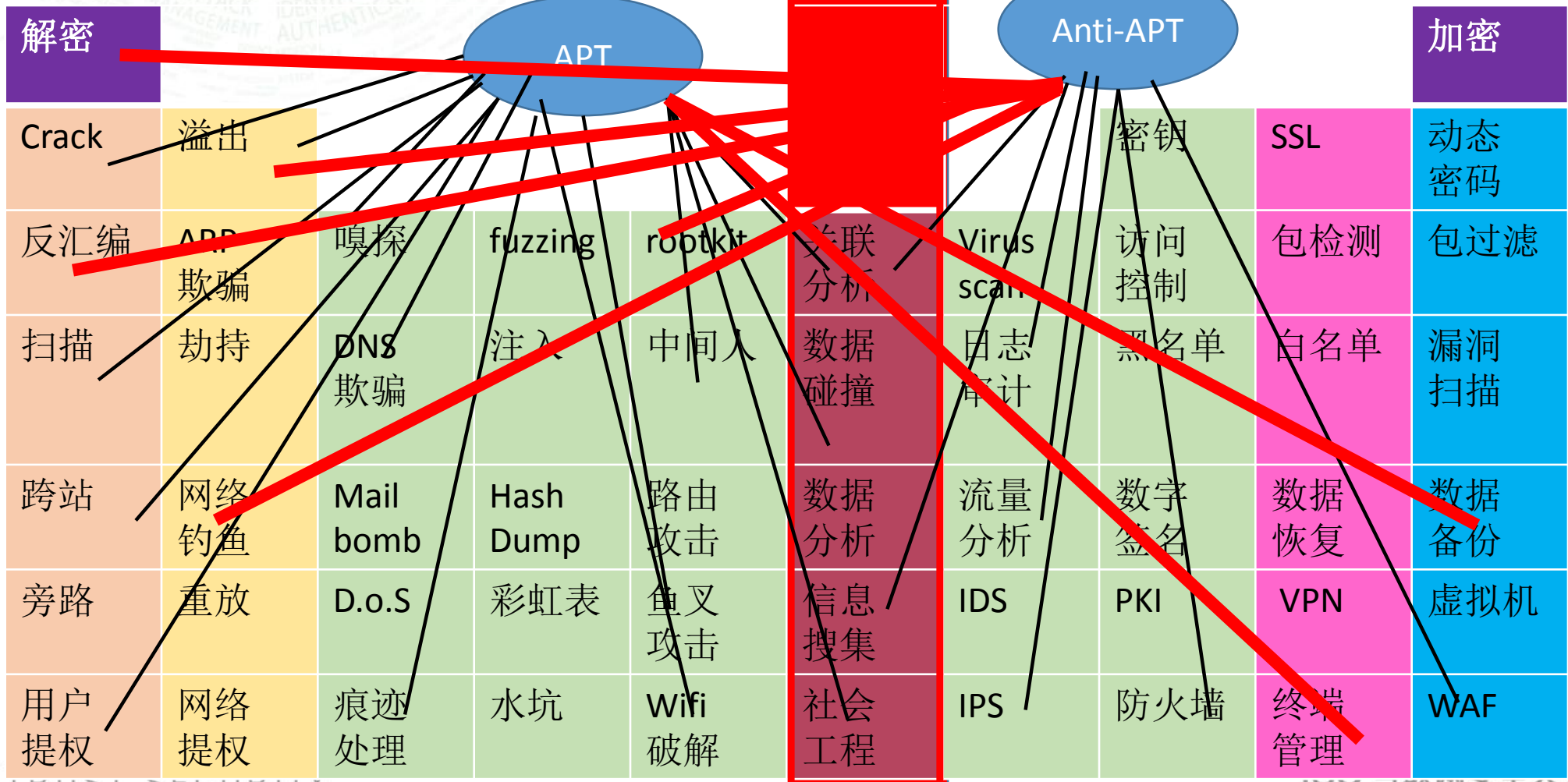
攻防两端的越界



进攻端元素

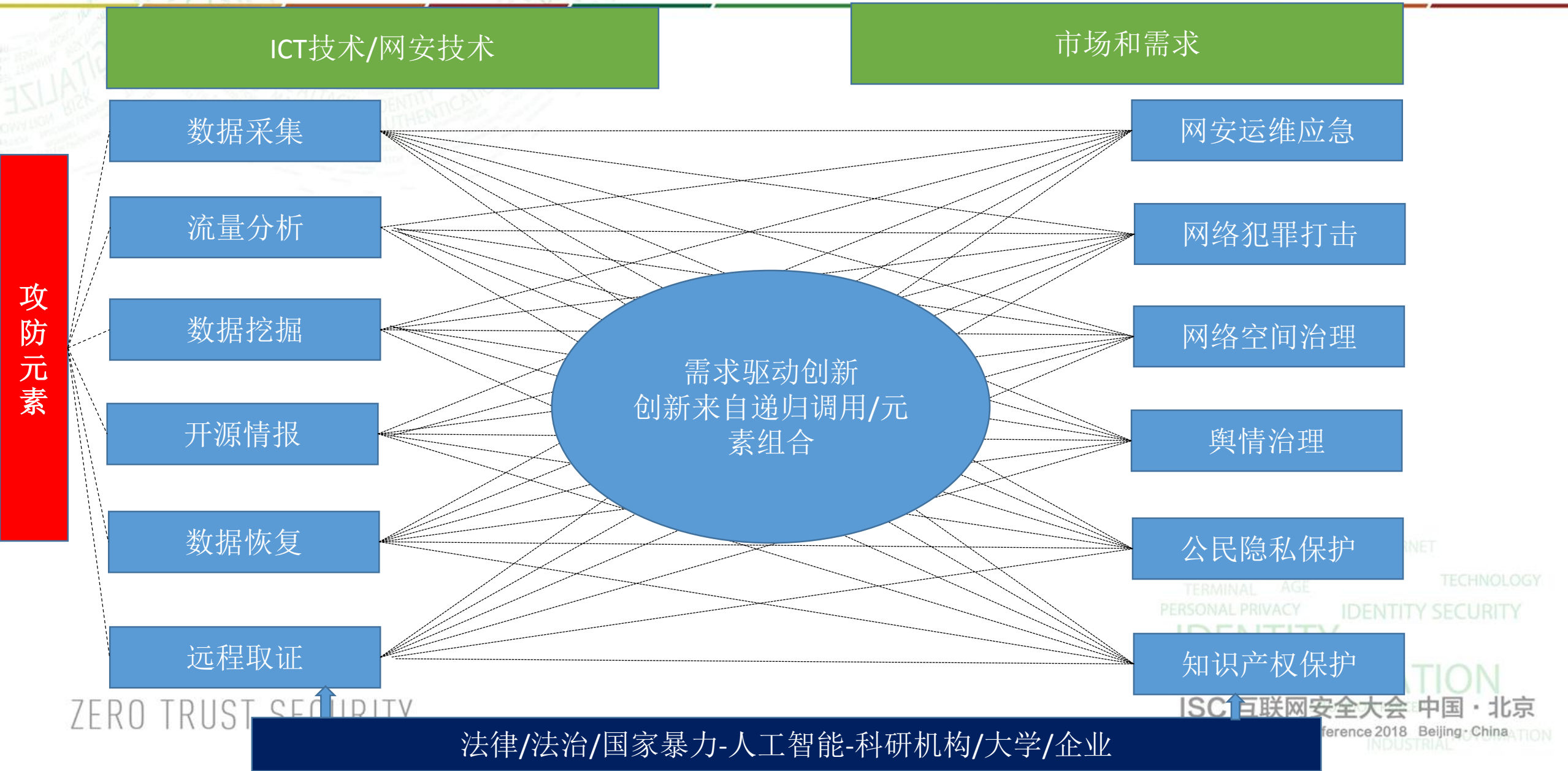
交叉元素

防守端元素



ZERO TRUST SECURITY

创造安全新作用





ISC 互联网安全大会



360互联网安全中心

谢谢！

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