Certificate Root Stores - An Area of Unity or Disparity?

Jegan Purushothaman, Ethan Thompson, AbdelRahman Abdou
Background

- Certificates
- Certificate Issuance
- Certificate Validation
- Certificate Root Stores
Our Work
Focus

- # of unique certificates
- # of unique organizations
- Inclusion policies
- Method of delivery
- Certificate usage
Focus

- # of unique certificates
- # of unique organizations
- Inclusion policies
- Method of delivery
- Certificate usage
Root Certificate Overlaps

- Total of 503 unique certificates
- 25% overlap between vendors

| Vendor  | # of Certs | # Exclusive |
|---------|------------|-------------|
| Microsoft | 432       | 247         |
| Apple   | 159       | 7           |
| Mozilla | 158       | 10          |
Root Certificate Overlaps

| Vendor | # of Certs | # Exclusive |
|--------|------------|-------------|
| Mozilla| 158        | 10          |
| Ubuntu | 127        | 0           |
| Android| 156        | 11          |
Organization Overlaps
Root Organizations Overlaps

| Vendor | # of Orgs | # Exclusive |
|--------|-----------|-------------|
| Microsoft | 133 | 69 |
| Apple | 59 | 0 |
| Mozilla | 55 | 2 |
Root Organizations Overlaps

| Vendor  | # of Orgs | # Exclusive |
|---------|-----------|-------------|
| Mozilla | 55        | 2           |
| Ubuntu  | 51        | 0           |
| Android | 53        | 1           |
Government Organization Overlaps
Policies

Microsoft

Apple

Mozilla

Ubuntu

Android
Impact of Root-Store Differences on Leaf Certs

|                      | Microsoft | Apple  | Mozilla |
|----------------------|-----------|--------|---------|
| Total Certs Trusted  | 585,595   | 585,567| 584,854 |
| Exclusively Trusted  | 26        | 1      | 0       |
Conclusion

- Despite the Censys data, trust disparities remain concerning
- Some differences are expected
- Left with questions
